DOCUMENT RESUME

ED 192 753 IR 008 822

TITLE A Study in Computer Abuse.
INSTITUTION Caulfield Inst. of Technology (Australia).
PUB DATE Feb 79
NOTE 95p.; Page 16 may not reproduce.

EDRS PRICE MF01/PC04 Plus Postage.
DESCRIPTORS Case Studies; Computer Programs; *Computers; *Crime; Foreign Countries; *Identification; *Prevention; Problems; State of the Art Reviews; Tables (Data)
IDENTIFIERS *Australia

ABSTRACT

Computer abuse is examined as both a general issue and as a specific problem. A statistical profile of computer crime lists distribution by country of reported cases, by industry of occurrence, and by amount of monetary loss. The characteristics of computer abuse are described along with the important categories of such crimes. Factors inhibiting reports of abuse, and the job positions of the perpetrators are also presented. Specific examples of abuse are cited from several countries, and nine Australian cases are briefly recounted. Prevention is discussed as a function of the types of controls employed in both the applications and the administrative areas. (Application controls cover all phases of data processing, while administrative controls deal with scheduling personnel, physical security, billing procedures, and maintenance and disaster procedures.) Problems in detecting computer crimes are also discussed, and some of the methods used are indicated. (BK)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED192753

U S DEPARTMENT OF HEALTH,
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

A STUDY IN COMPUTER ABUSE

Consisting of a research paper commissioned by CIT-CARB and a select bibliography of further reading on the subject published since 1975.

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY
Alan Hamstead

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

February 1979

IR008822

Cataloguing in Publication Data - CIT Library

Lewens, Alan

A study in computer abuse : consisting of a research paper commissioned by CIT-CARB / (Alan Lewens); and a select bibliography of further reading on the subject published since 1975 (compiled by Jean Gourlay) - (Caulfield, Vic. : Caulfield Institute of Technology), 1979.

vi leaves, 86 p. : ill.; cm. - (Caulfield Institute of Technology. Computer Abuse Research Bureau. Paper: no.1)

ISBN 0-909176-05-1
1. Computer crimes. 2. Computer crimes - Bibliography. I. Gourlay, Jean. II. Title. III. (Series)

364.162

ISBN No. 0-909176-05-1

INTRODUCTION

The first section of this publication is a Research Paper commissioned by CIT-CARB as an attempt to establish a profile of computer abuse as it now stands overseas, and to point to the latest means of prevention and detection.

I believe that this work is the foundation for more Australian research which was why CIT-CARB was set up in August 1976 to act as a resource centre and to carry out research into all aspects of computer abuse.

Its specific objectives include:

- to research computer crime profiles in Australia;
- to develop a taxonomy of preventative means;
- to investigate system integrity;
- to conduct seminars, conferences and workshops;
- to act as a focal point for the collection of hard data.

By bringing the problem to the eyes and ears of the Australian Business Community, a significant contribution to control of the problem and a healthier business operating climate will be established.

The second section is a select bibliography of the many books and articles on the subject published since 1975 and available in Australian Libraries.

The Computer Abuse Research Bureau at Caulfield Institute of Technology is indeed indebted to the work of CIT-CARB Researcher, Alan Lewens, to the funds from the David Syme Business School at C.I.T. and to the work of Mrs. Jean Gourlay who compiled the bibliography.

KEVIN J. FITZGERALD
Executive Director
CIT-CARB

CAULFIELD INSTITUTE OF TECHNOLOGY

COMPUTER ABUSE RESEARCH BUREAU

The Bureau will eventually consist of 20 members. As at March 1979 the Bureau's personnel were:

The CIT-CARB Executives

Chairman:	Kevin Fitzgerald,	CIT-CARB Executive Director Senior Lecturer - Accounting Systems, The David Syme Business School, CIT.
Secretary:	Alan Hamstead,	Financial Controller, CIT
Members:	Martin Burrell,	Director, Manser Consultants.
	Bill Gibson,	Councillor, Australian Computer Users Association; EDP Manager, R.G.Gilbertson Pty. Ltd.
	Gardarshan Gill,	Lecturer - Auditing, CIT.
	David Goble,	Senior Lecturer - EDP, CIT.
	Jack Greig,	Senior Lecturer - Systems, CIT.
	Alan Lewens,	Former Computer Abuse Researcher, CIT. Supply Manager, Ajax Pumps Pty. Ltd.
	Arthur Lunt,	EDP Manager, Insurance Council of Australia.
	Francine McNiff,	Lecturer in Law, Monash University.
	Gerry Maynard,	Senior Lecturer - EDP, CIT.
	John Newton,	Systems Engineer, IBM.
	Max Nicholls,	Senior Consultant - Management Information Systems, W.D.Scott Management Consultants.
	Roy Paterson,	Vice Chairman, Victoria Branch, Australian Computer Society, National Manager - Management Services, Ferris Norton and Associates, Chartered Accountants.
	Martin Ralston,	Secretary Australian Institute of Systems Analysts (Vic.Branch), Systems Consultant Arthur Andersen & Co.(Chartered Accountants)
	Jeff Richards,	EDP Audit Manager, Commercial Bank of Australia Ltd.
	Barry Williams,	Manager Industry Marketing (Vic.Division) Computer Sciences of Australia.

Other industry representatives will be invited to join in 1979 until the 20 positions are filled.

Further Information on CIT-CARB can be obtained from:

Alan Hamstead
Secretary CIT-CARB
Caulfield Institute of Technology
P.O. Box 197
CAULFIELD EAST. 3145
AUSTRALIA.

CONTENTS

		Page
SECTION 1. CIT-CARB Research Paper No.1		
1.	Introduction.	1
2.	Recommendations for Further Research.	3
3.	General Conclusions.	4
4.	Computer Abuse - What is it?	6
5.	Computer Abuse - Statistical Profile	6
6.	Characteristics of Computer Abuse	10
7.	Specific Examples of Computer Abuse	16
8.	Prevention.	22
9.	Detection	43
10.	Bibliography	62
SECTION 2. A Select Bibliography of further reading.		66

SECTION 1.

CAULFIELD INSTITUTE OF TECHNOLOGY

COMPUTER ABUSE RESEARCH BUREAU

Paper No. 1

Co-Ordinator: Kevin Fitzgerald

Author: Alan Lewens

1. INTRODUCTION

This paper is an attempt to cover a lot of ground in little depth; to gain an initial impression of the 'status quo' relating to computer abuse.

I do not apologise for the heavy use of the first person in this paper. I neither pretend to be an expert in the field, nor that the amount of research done has been adequate to make me so. The paper is essentially a subjective evaluation of the written material that I have been able to find. The quality of the evaluation is obviously open to question in view of the gaps in my knowledge. Nevertheless I am hopeful that I have provided a reasonably substantial base from which clear decisions can be made as to the direction of future research and the resources required for that research.

Under whatever banner, computer crime, fraud or abuse has become a scare-all in recent years, prompting a good deal of discussion, a lot of press coverage, and some modifications to the housing of computers and to the design of hardware and software. Nearly all of this heat has radiated from the U.S. since the reported incidence of computer abuse in Australia has been very low. It thus becomes very difficult to put computer abuse in any sort of proper perspective. I believe however that in generalized terms the whole area is in something of a mess.

Auditors are frequently conscious of the unsatisfactory control enforced by clients and of their own unsatisfactory audit techniques. They fear the possibility of being sued for negligence in not detecting significant fraud within a client organisation, whilst at the same time their own lack of expertise, or fear of reducing their client base, prevents them from radically improving the situation. Quite apart from which the situation in anything other than the largest organisations is more often than not incapable of significant improvement as things currently stand.

Hardware manufacturers are possibly capable of producing more secure systems but they would tend to reduce efficiency and flexibility of operations. The market has shown little sign of wanting such a change. Meanwhile the manufacturers tend to be shy about public discussion of computer abuse since it may reflect upon their systems. The attitude is frequently one of 'we are researching the problem and developing our technologies but it's mostly up to the user to show interest.'

Software is only as secure as its environment. Computer bureaux are often reluctant to discuss the matter since they are in the business of supposedly selling a 'secure' service, knowing that there is no such thing and aware that attempts to breach 'secure' systems might be encouraged by too much public discussion of computer abuse. They are in the business of trying to do the best with the means at their disposal, hoping that they are not faced by too sophisticated a villain. In their view then - the less said the better since it would only require one significant breach to do considerable damage to their market image. This is not however a realistic way of approaching the problem as a whole since it is of no use to those most in need - the users with their own facilities.

Users are commonly (perhaps I should say 'still') composed of EDP and general management. General management tends to be blissfully ignorant of the capabilities, limitations and risk exposures associated with their EDP systems and consciously or subconsciously seem to strive to stay that way. What they are concerned with is efficiency and operating cost. Hence the EDP manager, whilst he may be aware of the dangers faced by the organisation won't always feel like sticking his neck out to try and convince management to spend more on tighter controls and better preventative measures.

The general attitude is one of either technical advances or, someone else will solve the problem. Australia is looking to the U.S., but is that a reason for our burying our heads in the sand and remaining ignorant ourselves? I believe it is time to take the first few steps in the direction of educating those who need to know.

2. RECOMMENDATIONS FOR FURTHER RESEARCH

1. CIT-CARB should arrive at its own definition of 'computer abuse' to ensure that further work is founded on a reasonably solid conception of what everyone is talking about.

2. The Bureau should consider sending a questionnaire to leading computer users in Melbourne and Sydney in an effort to gather more details on an anonymous basis.

3. Internal and external auditors should be asked to comment on the usefulness of computer audit techniques known to them.

4. Work should be undertaken to evaluate risk exposure by type of industry and size of company. This could then be linked to the development of more specific preventative measures and better detection techniques.

5. CIT-CARB should fully document all possible exposures and monitor preventative measures available and any efforts being made to improve such measures.

3. GENERAL CONCLUSIONS

The conclusions I present in this section are largely unsubstantiated by hard data. Therefore an important area for further research is to assess their validity.

i. Computer technology and applications in Australia are at a level of sophistication very much on a par with the U.S.

ii. Computer abuse is evidently a growing risk in the U.S. and has the same relative potential in Australia.

iii. Computer abuse is a term which is simultaneously not only trendy and overdramatised but also representative of a very real weakness in computer applications. Moreover it is a weakness that is not generally appreciated.

iv. Computers cannot be made 100% secure.

v. Computer abuse is largely preventable by means of widely published control measures. These measures hinge predominantly on:

segregation of duties;
checking and control of input, output and operations; and
control of physical access.

vi. The predominant function of auditors is to check the proper existence of such preventative measures and controls.

vii. Such controls are adequately enforced only by a tiny minority of computer users. It may be that for the majority such controls are largely uneconomic or operationally too inefficient.

viii. If controls are found to be inadequate in an organisation, computer abuse becomes possible or even probable.

ix. There are <u>no</u> effective measures for the detection of some computer abuse.

x. No detective measures = no apparent loss
No apparent loss = insufficient control

Insufficient control → Risk of computer abuse ← No detective measures

xi. Increased protection may come from:

* more secure hardware/operating systems as a standard product;
* the development and widespread use of 'secure' software packages → phasing out of independent programmers;
* improved detection/auditing techniques;
* significant computer abuse leading to the suing of an external auditor and the consequent tightening of audits and required control measures.

xii. The problem - potential or actual - is significant.
Its solution requires co-ordinated action concentrating on:

hardware/operating system design;
software design;
user controls;
audit requirements and techniques; and
detection techniques.

These are distinct yet related areas which spread across different industries.

xiii. C.I.T. is uniquely positioned to take advantage of the demand for leadership in this area. Effective leadership will require:

* consistent application of research resources;
* consistent operation as a communications centre for the reception of information;
* diplomatic handling of areas of conflict between interested parties in the initial stages, a 'toned-down' style of publicity aimed at attracting those who know what they are talking about and can put in, rather than those who would 'waste' resources by taking out.

xiv. Computer abuse is an area in which it is easy to attract a lot of publicity in the short-run since it has 'lay interest', but difficult to maintain a good reputation over a greater period. It is only the steady building of a good reputation that will produce worthwhile results.

xv. Confidentiality would not necessarily enhance reputation. Leadership in this field would be consequent upon being first, having adequate resources and presenting an open, intelligent, informed approach. I believe that to give interested parties access to all material available would considerably enhance the building of 'leadership' statue.

xvi. Success for C.I.T. in becoming an Australian leader in this field would bring with it a position of influence in setting standards for auditors, computer suppliers and users. This would be a particularly heavy responsibility requiring a very high standard of professional behaviour on the part of C.I.T.

4. COMPUTER ABUSE - WHAT IS IT?

Computer Crime, Fraud and Abuse are common terms which are frequently confused and statistics may be misinterpreted accordingly.

Donn Parker ("Crime by Computer" 1976) tends to use 'Abuse' as a synonym for 'Crime' and states:

"Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could have suffered a loss and a perpetrator by intention made or could have made gain. Any incidents are identified as computer abuse if there is information to be gained by studying such incidents that will make computers safer in the future."

Brandt Allen ("The Big Computer Frauds: Lessons for CPA's") The Journal of Accountancy (May, 1977) states .....

"For purposes of this article, computer fraud is defined as any defalcation or embezzlement accomplished by tampering with computer programs, data files, operations, equipment or media, and resulting in losses sustained by the organization whose computer system was manipulated. In most instances, this would encompass all activities in the computer department as well as those departments that directly enter or prepare computer input. Excluded are thefts of computerised information, use of computer time for personal gain, alteration of computer records for nonfinancial gain and schemes where the employer was not the victim".

These definitions aim at slightly different areas, but I find both to be highly unsatisfactory in terms of providing us with an objective, repeatable, delineation of the features which would characterise 'crime', 'abuse', or 'fraud' in relation to the future.

5. COMPUTER ABUSE - STATISTICAL PROFILE

Country or Origin

Australian data is very sparse and this may be for a number of reasons such as:

i. there is no general idea of what is meant by 'computer abuse' or 'computer crime' so that incidents may be classified under another heading;

ii. Donn Parker:
"Research in criminology reveals that 85 per cent of all known crime goes unreported. There is reason to believe that a higher percentage of computer related-crime goes unreported. Victims tend not to report computer related incidents because of the great amount of publicity they generate, which often has an adverse effect on their business. Also, they often discover that they do not know how to correct a vulnerability.";

iii. controls in Australia are tighter, permitting less abuse;

iv. Australian perpetrators are smarter, permitting less detection;

v. Australians are more 'ethical';

vi. There is a small population of computers in Australia, which would naturally lead me to expect a small number of detected abuses.

Distribution by Country of Computer Abuse Cases (Donn Parker)

	Sept.1977		Sept.1977
U.S.A.	349	The Netherlands	2
U.K.	20	Belguim	1
West Germany	16	Denmark	1
Canada	11	Norway	1
France	10	Yugoslavia	1
Italy	10	Eastern Europe	1
Australia	4		
Sweden	4		
Japan	3		
South Africa	3		

Parker,

"The incidence of reported computer abuse relative to the number of computers .... is roughly 1 case per 10,000 computers in 1965 and 5 cases per 10,000 computers in 1975." (Parker - 1976)

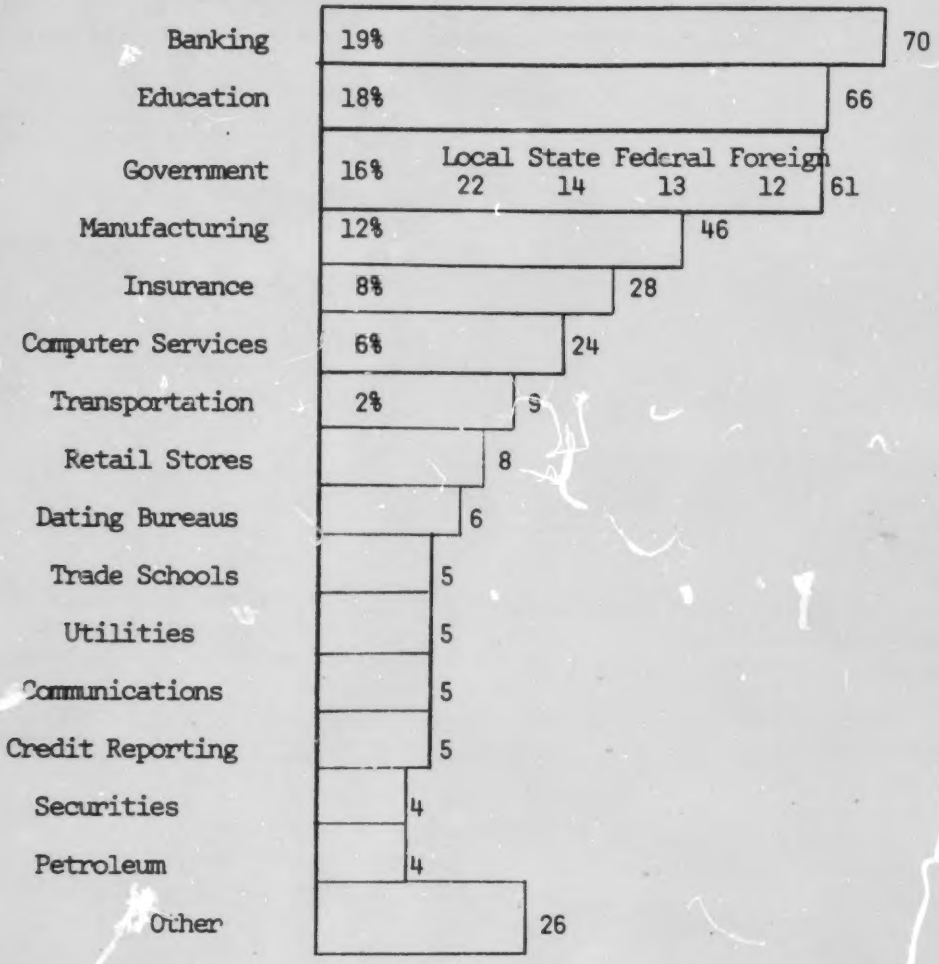
(The total U.S.A. population of computers is given as 200,000 in 1975) (The total Australian population of computers is given as approximate 10,000 in 1978).

Significantly, from a total of 374 reported cases in the U.S.A., 174 were able to be verified by Parker and SRI, and of those, 71 were discovered by including a 20 page questionnaire with each of 30,000 copies of Parker's report 'Computer Abuse'.

"Three hundred questionnaires were completed and returned, and among them were descriptions of 71 new computer abuse cases".

Of the remaining cases, 46 came from private sources, 42 from journals, newspapers and books, 13 from law enforcement agencies and 2 from unpublished documents.

COMPUTER ABUSE INCIDENCE BY INDUSTRY (372 Cases to October 1975)



Source: Stanford Research Institute.

$ Amount of Losses

Donn Parker:144 cases since 1963 yield simple average loss of $450,000
90 cases during 1974 average - $700,000

(Note: these figures are taken from Parker's 'Crime by Computer' and I would like to warn of dangers which appear to be associated with Parker's statistics:-

e.g. p.27 shows a table of 381 reported cases from 1958 to October 1975 with 69 for 1974;
p.29 shows a graph for losses in 144 verified cases from 1963 to September 1975 (excluding Equity Funding) with a total loss for the period of $65,000,000 and an average loss of $450,000;
p.32 shows a chart of 90 cases in 1974 giving a total loss of approximately $60,000,000 and an average loss of $700,000 approx).

Brandt Allen (May 1977) examined 150 cases of computer fraud, producing the following analysis of financial loss.

A. Average losses in computer frauds ($'000)

Type of Fraud	Corporation	Bank/Savings and Loan	State and Local Govt.	Federal Govt.
Payments to employees	$139	$3	$14	(
Payments to other individuals	133	-	487	($33
Payments to creditors	324	252	-	(
Accounting/ inventory control	1,300	195	-	(56
Collections/ deposits	43	157	-	-
Billings	6	-	-	-

B. Average loss, job position of perpetrator

Job Position of primary perpetrator	Total	No. Alone	Average Loss(000's) Alone	Total
Data entry/terminal operator	15	4	$8	727
Clerk/Teller	16	11	37	58
Programmer	15	10	20	53
Office/manager	21	18	274	314
Computer operator	9	5	33	37
Other Staff	5	4	48	92
Outside	5	3		696
Unknown	3	-		2,400
	89			

The 'total' for Data entry/terminal operator includes highly organized activities involving large welfare frauds and large inventory frauds. Brandt Allen does not clearly explain the large average loss in the 'unknown' category.

6. CHARACTERISTICS OF COMPUTER ABUSE

Donn Parker(1976) makes the following observation, on computer abuse "Two kinds of computer abuse were identified, termed 'inspec' and 'nonspec'. Inspec cases are those where computers were used within their correct specifications; there were no unauthorised acts directly against or in the computers. ...Nonspec types of cases involve those where the computers have been used in unauthorised ways not according to the specifications or instructions for their use".

He then makes the following comments:
"It is likely that fewer inspec computer abuse cases are reported than nonspec, because they are often not identified as being associated with the use of computers. For example, a survey was made of computer fraud within the federal government. A questionnaire was sent to a number of agencies asking them to report all computer frauds that have occurred in their organisations. One case was reported. The questionnaire instructions were changed to report all cases of fraud where data involved in the fraud may have entered a computer or come from a computer. This second attempt produced hundreds of cases from many of the agencies, and in one agency, literally thousands of cases."

Robert V. Jacobson ("Finding Hidden Computer Crime" Security Management April 1978) takes 115 cases of computer crime reported by Donn Parker/ SRI in "Computer Abuse" 1973 and finds that:
"Nineteen basic ways exist in which a data processing application can be manipulated to steal assets or to keep the system from functioning as intended, and there are two crimes aimed at computer systems, theft of services and computer sabotage. Theft of tangible items for their cash value has been omitted since this is not specifically a computer crime."

A. Twenty One Basic Computer Crime Categories

INPUT DATA

1. ADD FRAUDULENT INPUT DATA.
2. ALTER INPUT DATA.
3. OMIT INPUT DATA.

PROCESSING

4. MIS-POST TRANSACTIONS.
5. COUNTERFEIT OUTPUT.
6. STEAL MONEY IN MANY SMALL AMOUNTS.
7. SUPPRESS/ALTER OUTPUT SELECTIVELY.
8. ALTER OR ADD MASTER FILE RECORDS.
9. OVERRIDE INTERNAL CHECKS.
10. INTRODUCE DELIBERATE PROGRAM BUGS
11. PARTIAL POSTING OF TRANSACTIONS.

OUTPUT

12. DESTROY OUTPUT.
13. THEFT OF OUTPUT.
14. SUBSTITUTE COUNTERFEIT OUTPUT.

MASTER FILES

15. STEAL MASTER FILE INFORMATION.
16. DESTROY MASTER FILES.
17. INTER-CYCLE MASTER FILE TAMPERING.
18. "RANSOM" MASTER FILES.

MISCELLANEOUS

19. EXPLOIT INTER-SYSTEM DEFICIENCIES.
20. SABOTAGE THE COMPUTER FACILITY.
21. UNAUTHORIZED COMPUTER USAGE.

Jacobson then analyses the methods used in the 115 cases and finds that four account for 62%.

B. The Big Four Computer Crimes

	COMPUTER CRIME CATEGORY	% OF OCCURANCE
1.	ADD FRAUDULENT INPUT DATA	21%
15.	STEAL MASTER FILE INFORMATION	16%
20.	SABOTAGE THE COMPUTER FACILITY	15%
21.	UNAUTHORIZED COMPUTER USAGE	10%
	TOTAL	62%

To attempt to explain the high occurrence rate of these four he concludes that they are in fact very common and/or they are easily detected and/or they are generally published.

C. Analysis of the Big Four Crimes

		HIGH OCCURRENCE RATE	EASILY DETECTED	GENERALLY PUBLISHED
1.	ADD FRAUDULENT INPUT DATA	X	X	
15.	STEAL MASTER FILE INFORMATION	X		X
20.	SABOTAGE THE COMPUTER FACILITY		X	X
21.	UNAUTHORIZED COMPUTER USAGE	X		

He then details ten crime categories which only account for 11% of the total and attempts to indicate some of the factors influencing this as follows.

D. Factors Leading to a Low Published Crime Rate.

COMPUTER CRIME CATEGORIES	Limited Opportunity	Unattractive Crime	Undiscovered	Mis-identified	Publication Suppressed
Suppress or alter output			X		X
Alter master file(s)			X	X	X
Introduce deliberate bugs			X		X
Sabotage of files or output				X	X
Partial posting of transactions			X		X
Theft of output			X		
"Counterfeit" output		X			
Intercycle master file tampering			X		X
Theft of master file for "ransom"		X			
Interface deficiencies	X				X

Brandt Allen(May 1977)once again looking at fraud analysed 150 cases and found the methods of computer manipulation were:

Transactions added, altered or deleted	69%
Programme changes	9%
File changes	8%
Improper operation	3%
Miscellaneous, unknown	11%

He further analysed these by job position of perpetrator:

Job Position	No. of Total Perpet-rators	No. of Trans-actions Changed	No. of File Changes	No. of Program Changes	No. of Improper Operations	No. Misc/ Unknown
Data Entry/ Terminal Operation	15	13	1	-	-	1
Clerk/ Teller	16	15	1	-	-	-
Programmer	15	-	-	14	-	1
Office Manager	21	15	1	3	1	1
Computer Operator	9	5	1	-	3	-
Other Staff	5	2	1	-	-	2
Outsider	5	4	-	-	-	1
Unknown	3	1	2	-	-	-

Donn Parker "Computer Abuse Perpetrators and Vulneralities of "Computer Systems" (Stanford Research Institute U.S.A., 1975) analysed computer crime by type of loss:

Financial Fraud or theft	39%
Information on Property fraud, theft	25%
Unauthorised use or sale of services	18%
Vandalism	18%

He also analysed the functional vulnerabilities in 362 cases as follows:

POOR CONTROLS OVER MANUAL I/O HANDLING	41%
WEAK OR ABSENT PHYSICAL ACCESS CONTROLS	13%
WEAKNESSES IN COMPUTER AND TERMINAL OPERATION	12%
FAILURE OF BUSINESS ETHICS	11%
POOR CONTROL OVER COMPUTER PROGRAMS	9%
LACK OF OPERATING SYSTEM ACCESS CONTROLS AND INTEGRITY	7%
FAILURE TO PREVENT AND DETECT TIME-SHARING USING IMPERSONATION	5%
WEAK MAGNETIC TAPE LIBRARY CONTROLS	2%

E. In Perspective:

The SAC Report i.e. Stanford Research Institute ("Systems Auditability and Control - Control Practices", Institute of Internal Auditors, 1977) asked Data Processing and Internal Audit Staff which two of the following areas of potential loss exposure in the data processing department they were most concerned about. The results were:

	Percentage of Organizations Selecting Each Category	
	Data Processing	Internal Audit
Potential Loss from:-		
Errors and Omissions	61.8%	46.8%
Improper Controls	47.4	67.1
Inadequate systems design	43.3	41.2
Fraud and Defalcation	17.1	15.6
Failure to comply with standards	14.9	20.9
or Procedures	7.5	6.7
Inadequate Conversion methods	8.0	1.7
other		

There is a high incidence of collusion in computer crime. Max White of IBM Australia quoted an unnamed USA analysis as showing that .....

> "in more conventional fraud and embezzlement activity collusion in any major scale occurs in only a small number of cases (about 4%) whereas in computer - related embezzlement, it is significant in nearly 50% of the cases."

7. SPECIFIC EXAMPLES OF COMPUTER ABUSE

Brandt Allen (1977)

Long running computer frauds

Case	Summary	Amount (thousands)	Time frame (years)	Type of scheme	Computer manipulation	Fraudulent debit	Job position of primary perpetrator	Number of perpetrators inside/outside	Means of detection
1	Accountant at west coast department store set up phony vendors, purchases and vouchers.	$ 100	1.3	Disbursements	Unauthorized transactions added	Inventory	Accountant	1/-	Suspicious bank employee
2	Claims reviewer at insurance company prepared false claims payable to friends in a manner that would be paid automatically by the computer.	$ 128	4	Fraudulent claims paid	Unauthorized transactions added	Expense	Claims clerk	1/22	Error made by greedy associate
3	Clerk at storage facility entered false information to computerized inventory system to mask theft of inventory. Shipments then made without billing.	$ 4,000	6	Inventory/ billing	Input transactions altered	Inventory	Computer terminal operator	1/13	Physical inventory shortage detected in audit
4	Warehouse employees manipulated computerized inventory system through unauthorized terminal entries to mask inventory thefts.	$ 200	1.5	Inventory	Unauthorized terminal entries	None (inventory records changed as to location)	Warehouse employee(s)	"Several"	Suspicious wife of store manager
5	Accountant at metal fabricating company padded payroll, thereby extracting funds for own use.	$ 100	3	Payroll	Unknown	Expense	Accountant	1/-	IRS investigation
6	Officer of London bank stole funds from inactive customer accounts.	$ 290	5	Account transfers	Unauthorized addition and alteration of transactions	Customer accounts (liability)	Computer liaison officer	1/-	Unknown
7	Bank employee misused on line banking system to perpetrate large lapping fraud including unrecorded transactions, altered transactions and unauthorized account transfers.	$ 1,400	3	Lapping	Transactions altered, added and withheld	Customer accounts (liability)	Teller supervisor	1/-	Gambling activities uncovered by police raid
8	Manufacturing company manager who had designed and installed automated accounting system used it to steal.	$ 1,000	2	Disbursements (also billings fraud)	Transactions altered (also unauthorized transactions)	Inventory (also expense)	Operations manager	1/1	Suspicious associate
9	Customer representatives of large public utility, together with outside associate, erased customer receivables using computer error correction codes; received kickback from customer.	$ 25 (probable losses much greater)	2	Accounts receivable–collections	Unauthorized transactions	Expense (adjusting entry)	Customer service representative	2/1	Suspicious bank employee together with expanded type of scheme
10	Clerk in department store established phony purchases and vouchers paid to friend's company.	$ 120	3	Disbursements	Unauthorized transactions	Inventory	Accounts clerk	1/1	Suspicious associate
11	Organized crime ring operated check-kiting fraud between two banks using computer room employees who altered deposit memos to record check deposits as available for immediate withdrawal.	$ 900	4	Kiting (float fraud)	Transactions altered	(Timing)	VP-computer systems (also assistant branch manager)	2/3	Bank messenger failed to deliver checks on time
12	Accountant at large wholesaler established phony vendors through computerized accounting system that he operated.	$ 1,000	4	Disbursements	Unauthorized transactions	Inventory	Controller	1/-	Gave up
13	Officer of brokerage house misappropriated company funds through computer system that he controlled.	$ 277	3	Account transfers	Unauthorized transactions	Revenue account (interest earned)	VP-computer systems	1/-	Unknown
14	Partner at brokerage house transferred funds from firm's accounts to his own.	$ 81	3	Account transfers	Unauthorized transactions	Expense (via adjusting entry)	Partner-head of computer system	1/-	Unknown
15	Director of publishing subsidiary manipulated computer system to add false sales and block recording of accounts payable—all to improve operating results, thereby securing a position on board of directors.	$11,500	"Several years"	Padded sales (also unrecorded expense)	Program alterations (also file changes)	Receivables	Director of subsidiary	5/-	Unknown

New Yorker 1977:

Pacific Telephone and Telegraph Co. - $1 million
use of remote terminal to enter false order to cover theft of inventory.

Unnamed U.S. Banks - $2.0 million
"Common" use of input operator to transmit fraudulent transfer of $2.0 million.

Unnamed U.S. Banks - $1 million
Printed cheques with name of one bank and computer - read numbers of the other. Drew on cheques which bounced to and fro for weeks.

Penn Central Railroad - $X million
Manipulation of computer programme to divert 200 boxcars from Penn Central Sidings.

U.S. Army, Korea, 1970's - $18 million p.a.
theft of goods concealed by manipulation of inventory and supply programmes.

Exxon Corporation - $20 million
Manipulation jointly of oil guages and the computer.

Oil Co., Alaska - $X million
loss of bid for drilling rights - underbid following tapping of telephone link carrying information between geological team and the computer.

Insware Co. U.S.A. - $10 million
A tape librarian given 30 days notice erased, mislabelled or misfiled tapes.

IBM, San Jose - $600 million Trade Secret
IBM employee walked out with software under development.

A. Equity Funding

22 CONVICTIONS $114 MILLION BOGUS PROFIT

(1) 'INFLATED EARNING PHASE' 1964-68

BOOK ENTRIES OF BOGUS COMMISSION

→ INFLATED EARNINGS/TAXES

→ INFLATED 'ASSETS'

→ INFLATED SHARE VALUES

→ SEVERE CASH FLOW PROBLEMS

(2) 'FOREIGN PHASE 1968-70

FRAUDS LINKED WITH OVERSEAS OPERATIONS
BORROWINGS WITHOUT RECORDING LIABILITIES
SEVERAL ACQUISITIONS - TRASNFER & MANIPULATION OF FUNDS

(3) 'INSURANCE PHASE' 1970-73

PRODUCTION OF BOGUS INSURANCE POLICIES.

+ SALE OF INTEREST TO CO-INSURER.

→ NEED FOR INCREASING NO. OF BOGUS POLICIES FOR RESALE TO GENERATE CASH TO SUPPORT MYTH OF CO. WITH GROWING EARNINGS AND ASSETS.

→ 2/3 of 97,000 POLICIES BOGUS

→ USE OF COMPUTER

→ 1972 :- MINIMUM INCOME FROM FRAUD - $35.7 M.
REPORTED CONSOLIDATED EARNINGS - $22.6 M.

Penetration of Systems:

USAF Multics 'secure' time-sharing system designed by Honeywell Massachusetts Inst. of Technology	penetrated by Mitre Corp.
U.S. Defense Universe 1108 executive system	penetrated by 3 computer scientists from U.S. Naval Research Lab.

U.S.A.F. Major Robert R. Schell (New Yorker 22.8.1977):
"The problem lies in the fact that computers were designed to store information, not to safeguard it ... Computers just weren't designed with that purpose in mind .

B. Australian Cases

1. Computer Shot - Melbourne - Vietnam demonstrations.

2. (New Yorker 22.8.1977)
"A computer specialist employed by the Australian Taxation Commission is reported to have sold to people with income-tax forms to fill out, copies of documentation based on highly confidential computer logic, that described the computerised methods used by the commission to check on the legitimacy of taxpayers' claims for deductions.

3. (C & L Newspaper Cutting, 1978)
Sydney building society fraud discovered in 1976 by R. L. Combs, M.D. of Online Systems (Qld) Pty. Ltd. The firm lost between $30,000 and $40,000 but did not prosecute.
"The fraud involved use of an interest adjustment facility by an employee to credit large interest adjustments to his own and other fraudulent accounts."

4. (Daily News 26.2.1978)
W.A. Company Fraud Squad - Det. Sgt. Brian Bull
"We have not had a great deal of computer crime here yet, but there is a growing trend entering Australia from overseas through the Eastern States.
In W.A. so far there has been several computer frauds, but as yet they are only small."

5. (The Age 15.9.1978)
N.S.W. Attorney General Mr. Walker
"He said there were two cases in Australia under investigation ... a $1.1 million loss in building society funds in Queensland and a case in N.S.W. which he said he could not detail."

6. (Private Sources)
Melbourne Bank - No financial loss
Programmer left the bank but had left maverick instruction in a program. All but two of password controls were changed but he was able to access computer by remote dial up. Vigilant computer operator deduced that the computer was taking longer to process certain portions of the operating system.

7. A 30 year insurance company O & M analyst used a computer terminal to scan policies with large surrender values for the purpose of borrowing from them without the policy holder's knowledge. He did this by creating a new address for the mailing of the loan interest notice and the loan cheque. Loan details were then erased from the computer file. He was captured when a policy holder received a loan interest notice in error.

8. An input clerk in a government office created false computer input documents to reactivate payments to a disqualified social security benefactor. His action was discovered by two fellow employees who demanded money for their silence. Further false social security payments had to be raised in order for the blackmail money to be paid. Almost $5,000 was raised by the input clerk in the five weeks that the scheme lasted. All involved were apprehended, forced to pay restitution and fined with prison if in default.

9. A government output clerk with access to a master file of names and addresses of social security beneficiaries inserted false particulars into the computer file thus inducing the issue of cheques payable in false names. A total of approximately $130,000 was fraudulently obtained by the output clerk and one outsider accomplice over three and a half years. Both were convicted and sentenced to two year's imprisonment.

C. Some Specific Types of Crime

1) TROJAN HORSE

METHOD : - IN HIERARCHIAL SOFTWARE STRUCTURE EMBED AN INSTRUCTION GIVING CONTROL OVER PRIVILEGED APPLICATIONS INTO NON-PRIVILEGED PROGRAM. INCLUDE INSTRUCTION FOR ERASURE OF ALL EVIDENCE. AWAIT USE OF PROGRAMME BY PRIVILEGED PERSON IN PRIVILEGED MODE.

VICTIM : - U.S.NAVY AND OTHERS INCLUDING U.S. UNIVERSITY

DETECTION:- CORE DUMP & ANALYSIS

= REASONABLE SUSPICION !

PREVENTION : - M/C SUPERVISION OF SUSPECT INSTRUCTIONS IN PRIVILEGED PROGRAMMES.

2) ROUNDING

METHOD :- ACCUMULATE DECIMAL CENTS GAINED FROM ROUNDING DOWN INTO PERSONAL ACCOUNT

VICTIM :- U.S. BANK

DETECTION :- (a) CHECK ALL INSTRUCTIONS IN THE PROGRAMME (MAY BE WELL DISGUISED)

(b) RE-CALCULATE THE INTEREST FOR THE PROGRAMMER'S ACCOUNT.

3) TIME BOMB

METHOD : - INSERT INSTRUCTION IN PROGRAMME TO (E.G.) DESTROY DATA RECORDS IF PAYROLL NUMBER CEASES TO APPEAR.

VICTIM : - FRENCH CO.

DETECTION : - (a) MAPPING = LIST OF UNUSED SEGMENTS

(b) CHECK ALL THE INSTRUCTIONS IN THE PROGRAMME.

8. PREVENTION

Prevention of Computer Abuse is covered by the term 'CONTROL'. There are several comprehensive guides, among the most important being:

Canadian Institute of Chartered Accountants:
'Computer Control Guidelines' 1970

Institute of Internal Auditors
'Systems Auditability and Control- Control Practices' 1977

Mair, Davis & Wood (Institute of Internal Auditors)
'Computer Control and Audit' 1976

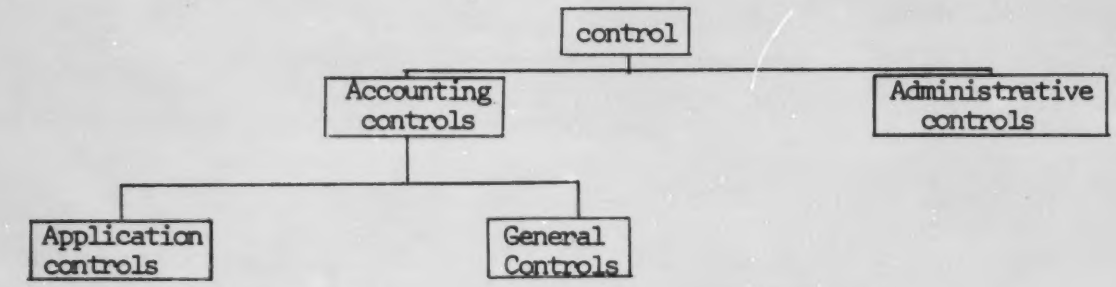
Porter & Perry
'EDP Controls and Auditing' 1974

Australian Computer Society - Exposure Draft 1976
'Comprehensive E.D.P. Security Guidelines'

These effectively cover a very broad area associated with Computer Control and Security and there is very little point in trying to compete with or add to what has already been written.

However it should be possible to give some indication of the ground covered by 'Computer Control'; so firstly I have attempted to summarize some of the major points made by Porter and Perry (1974) then I have followed this with a listing of the ground covered by the SAC (1977) study.

Porter and Perry show the overall system of control in a schematic form as follows.



- Accuracy
- Completeness

- organisation
- procedures and standards
  - . Programme changes
  - . Systems development
  - . EDP facility

In more detail:

Application controls
- involve controls over transaction data - data oriented

Administrative and General controls
- policy and procedures - procedure oriented

A. EDP Administrative and General Controls

Functions may be devided into two main areas:

(1) systems and Programming,
control over the implementation of new systems, changes to existing systems programming standards and documentation guidelines;

(2) operations,
controls over operating practices, data storage, physical security, record construction procedures, backup facilities and emergency procedures. The input-output control function is important to ensure that specific tasks are carried out effectively and efficiently. The control function acts as an interface between the data processing department and the user department.

B. Application Controls

These serve purposes associated with prevention, detection and correction to ensure that the recording, classifying and summarizing of authorised transactions and the updating of master files will produce accurate and complete information on a timely basis. This means assurance that:

(1) all authorised transactions are completely processed once and only once;

(2) transaction data are complete and accurate;

(3) transaction processing is correct and appropriate to the circumstances;

(4) processing results are utilised for intended benefits; and

(5) the application can continue to function.

In Preventative control areas covered will include:

source data authorisation;
passwords or other verification of right of access;
data Conversion;
source-date preparation;
turn-around Document;
pre-numbered forms;
input validation;
computer up-dating of files; and
controls over processing.

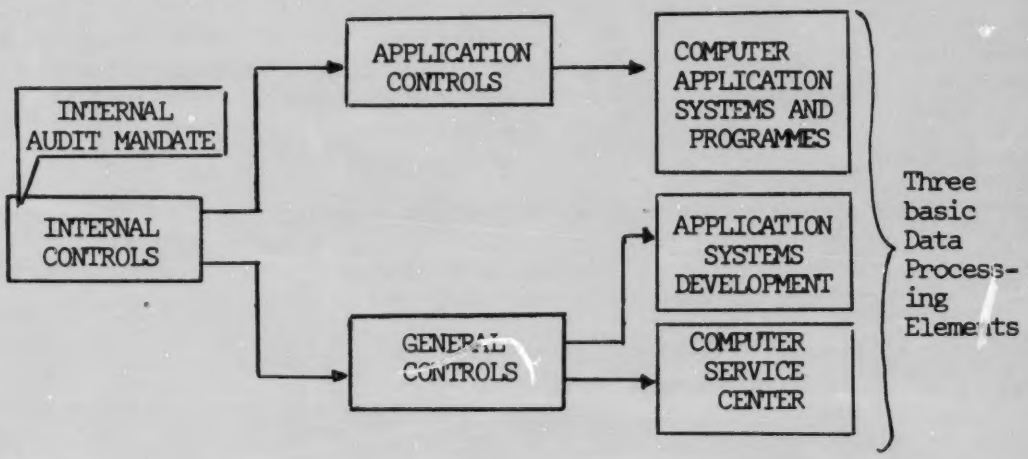
Detective Controls include :

data transmissions;
control register;
control totals;
documentation and testing;
labels; and
output checks.

Corrective Controls assist in the investigation and correction of causes of exposure that have been detected and include:

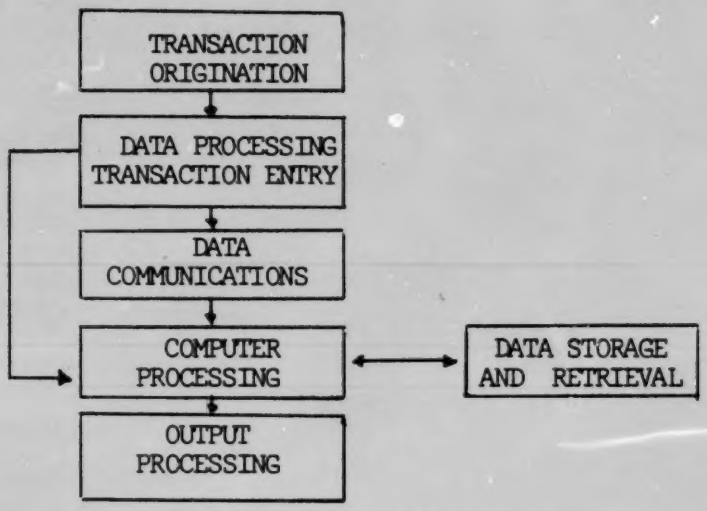
audit trails;
error detection and submission;
discrepancy reports; and
backup and recovery.

The SAC study shows control as:-



INTERNAL CONTROL RELATIONSHIP

Then Application System Controls are broken down into those covering six areas,



SCHEME FOR CLASSIFICATION OF APPLICATION SYSTEM CONTROLS

Tables for these areas are as follows :

TABLE 8.1

TRANSACTION ENTRY CONTROL STRUCTURE

Control Area	Control Type	Control
Transaction (batch) data entry	Written procedures	Control documentation
		User procedures
	Physical hardware	Location of data conversion operation
		Simultaneous recording
Terminal data	Terminal software features	Security of data entry terminal
		Interactive display
		Computer-aided instruction
		User application system access
		Terminal authority levels
		Data access matrix
		Master commands
		Terminal sign-on procedures
		Review of terminal assignments
	Hardware control features	Terminal features
		Intelligent terminals
Transaction data validation	Transcription verification techniques	Key verification
		Preprogrammed keying formats
	Data content validation	Editing and validating routines
		Transaction data cutoff
		Passwords
Batch proof and balancing	Data input controls	Processing schedules
		Turnaround documents
		Cancellation of source documents
		Logging
	Proof and balancing methods	Manual check of control figures
		Batch control
		Batch header records
Transaction entry error handling	Error detection	Error display
		Unauthorized access attempts
		Error listings
	Error correction	Corrective action
		Warning messages
		Error message
	Corrected data resubmission	Corrected data editing
		Control totals and rejects

TABLE 8.2

TRANSACTION ORIGINATION CONTROL STRUCTURE

Control Area	Control Type	Control
Source document origination	Written procedures	Control documentation User procedures and manuals
	Source document design	Special purpose forms Source document numbers Transaction identification Cross reference Sequence log
	Source document storage	Restricted access Accountable source document storage Intermediate storage and transportation
	Source document handling	Dual custody
Authorization	Source document preparation	Separation of duties Signatures
	Written procedures	Written authorization
	Approval of source documents	Evidence of approval Transaction conflicts matrix
Data processing input preparation	Transaction identification	Transaction numbering User identification Schedule desk
	User review of input	Manual review
	Batching	Batch serial number Limit the number of transactions in a batch Batch and balance source data at point of origin
	Logging	Logs of source document transmittal between organizations
	Transmittal	Transmittal document Mail and message carrier Physically secure input
Source document retention	Source document retention characteristics	Source turnaround Retention dates on source documents Source document storage index
	Filing of source documents	File of source documents Batch storage Source documents maintained at origin
	Retention storage	Filing in user areas Limited access to retention facilities Removal from retention

TRANSACTION ORIGINATION CONTROL STRUCTURE Contd.

Control Area	Control Type	Control
Source document error handling	Error procedures	Written error handling procedures Source document correction procedures Responsibility for error correction
	Error detection	Error logging Visual review of source documents
	Error correction processing	Error notification Identification of error correction
	Corrected data resubmission	Verification of re-entered data Monitoring of error corrections

TABLE 8.3 29

DATA COMMUNICATION CONTROL STRUCTURE

Control Area	Control Type	Control
Message Input	Hardware related	Electronic identification code
	Software and procedure related	Secure phone equipment rooms
		Network configuration polling table
		Sending message identification
		Security table
		Communication system control log
Message transmission	Hardware related	Communication line routing
		Line conditioning
		Automatic store and forward
		Automatic dial backup
		Modem loop-back switch
		Forward error correction
		Validity check
		Echo checking
		Message intercept function
		Packet switching networks
		Local loop security
		Encryption techniques
		Multipurpose modems
		Backup modems
		Backup lines
	Software and procedure related	Transmission batch controls
Message reception and accounting	Hardware related	Detection with retransmission
		Backup electrical power
	Software and procedure related	Validation
		Line usage records
		Message sequence number
		Input/output message log
		Dial-up modems
		Message backup log
		Error recording procedures

TABLE 8.4

COMPUTER PROCESSING CONTROL STRUCTURE

Control Area	Control Type	Control
Computer process integrity	Transaction identification	Transaction codes
		Monitoring of computer-generated transactions
	Computation and logic	Control totals
		Default option
		Anticipation control
		Dual Fields
		Arithmetic accuracy
		Exception reporting
		File control totals
		File completion check
	File maintenance	Balancing the computer file
		Dummy records
	Computer operations personnel	Operator instructions
		Computer program run books
		Computer console
		Display messages
Computer processing error handling	Error reporting	Error reporting
		Batch control header balancing
		Production report of rejected conditions
	Error correction	Automated error suspense file
		Discrepancy report
		Error serial numbers
	Corrected data resubmission	Destructive update
		Error suspense re-entry.

TABLE 8.5

DATA STORAGE AND RETRIEVAL CONTROL STRUCTURE

Control Area	Control Type	Control
File handling	Library	Operating procedures
		On-line library
		Source program statement library
	File access	Conflict prevention feature
		Group files
		File classification
		Data base control table
		Passwords
		Program linkage control table
		Header/trailer labels
		System inquiries
		System logging
		Manual authorization of security table
		Program modification
	File maintenance	Folio number
		Before and after looks
		Masterfile changes
		Dormant files
		Excessive activity
		Scanning of critical files
	Backup	Activity tape
		Separate computer
		Copy masterfiles
		Backup procedures
		Disaster plan
		Recovery procedures
File error handling	Error reporting	Operator intervention
		Comparison programs
	Error correction	Restart procedures
		Backup file usage
	Correction reentry	Job stream log

TABLE 3.6

OUTPUT PROCESSING CONTROL STRUCTURE

Control Area	Control Type	Control
Data processing balancing and reconciliation	Data processing control group	Reconciliation Transaction log Computer console log Systems output logs Record of output reports Monitoring process flow Job control card review Graphical charts
Output distribution	Output handling	Handling procedures for computer output Output report distribution Report copies
User balancing and reconciliation	Monitoring procedures	User department changes in masterfiles Report heading Transaction tracing list Internally generated transactions Control totals
	Testing procedures	Statistical sampling of final report List of all transactions
Records retention	User retention and disposal methods	Waste disposal procedures Deletion of unused reports
Accountable documents	Accountable document handling	Negotiable documents storage Printing of additional sequence number on preprinted forms
Output error handling	Error reporting	Independent history file of errors Aging open items Error logging by control groups Output activity review
	Error correction	Error correction processing Identification of error correction Correction procedures Responsibility for error correction
	Correction re-entry	Error logging Verification of re-entered data Monitoring of error conditions

General controls are then listed for the control of the Computer Service Centre and Application Systems Development

COMPUTER SERVICE CENTER CONTROL STRUCTURE

Control Area	Control
Input/output scheduling and control	Input/output control group Job handling procedures Scheduling procedures Processing schedules Cutoff dates Job submission/authorization Input/output control group Daily work schedules
Media library controls	Access controls File release Separate library area Physical security Media restriction issuance Media inventory control procedures Media restriction quantity Media use records Handling equipment Security vaults Temperature and humidity control Off-site storage Duplicate file storage Redundancy and backup procedures
Malfunction reporting and preventive maintenance	Procedures reporting Problem documentation System utilization report System utilization reports review Vendor failures logging Resolutions problem logging Trouble reporting responsibility
Environment controls and physical security	Physical security Access controls Backup for power, cooling, etc. Software backup Hardware backup
Separation of duties	Separation of duties within data processing Separation of data processing from other organizational units. Computer programs to enforce separation between systems Automated controls to separate on-line users
Resources planning	Plan for facilities, equipment, software, and personnel Variance between actual and planned goals
User billing/charge-out procedures	Service contracts between the user and data processing Procedures to arbitrate disputes Chargeable versus free services Billing procedures tied to the computerized job accounting system

Control Area	Control
	Billing algorithm, periodic user billing statements, rerun cost allocation procedure
Disaster recovery	Disaster plan Disaster scenarios to update the disaster plan Top management's commitment to the disaster plan Maintenance and updating of the disaster plan User responsibility for the disaster plan Testing of the disaster plan User training in use of the disaster plan

APPLICATION SYSTEM DEVELOPMENT CONTROL STRUCTURE

Control Area	Control
System development life cycle	Review user requirements Review project organization Review hardware requirements Review internal controls Require user or internal auditor sign-off Review detailed design documents Review file requirements Review costs and schedules Review test plan Review user and operational documentation Review test results Require user and internal audit sign-off Review conversion plan Review adequacy of documentation Identify user problem areas Identify system development problems
Project management	PERT control technique
Structured programming	Audit trail
Acceptance testing	Comparison of base case data to system produced data Manual review of output reports
Programme change control	Require formal written request Review all changes Use of change control committee Restrict number and type of persons who make changes Require operator and programmer to make changes Modify SMF to obtain reports of all changes to load libraries Require report of quick fixes Limit number of times changes are made per time period Use programme packages to control access to source libraries
Documentation	Provide flow of all application system data flow Specify how the programmes implement controls Specify how programmes are to be operated backed up, and recovered Maintain up-to-date changes to accepted documents Specify allowable user commands and functions
Data base administration	Develop standards Establish and monitor standards Document and provide procedures to control operations Measure effectiveness of performance and integrity controls Develop security/control education programmes

Brandt Allen (May 1977) identifies six main concerns in preventing computer fraud.

1. Transaction Controls - the need to tighten controls over the generation and flow of input transactions.

2. Rigorous audits - particularly in defining the causes of inventory losses

3. Improved responsibility reporting - "the most effective internal control for the big cases seems to be improved management reporting systems to alert others to possible fraudulent transactions."

4. Programme Controls - independent verification of critical programmes and supervision of secure file storage.

5. File Controls - require a file librarian who is responsible for the security of all critical programme and data files.

6. Place EDP low in order - "The auditor can do a great service for his client and for himself by working to reduce the 'management by crisis' conditions found in many computer rooms."

Robert Jacobson looks at effective means of prevention in terms of five basic security measures.

	Physical Access Controls	Normal Input Controls	Resources Access Controls	Software Change Control	Independent Checks
THE BIG FOUR					
Add improper input items	X	X		X	X
Info. theft via master files	X		X		
Direct attack, sabotage	X			X	
Unauthorized access/use	X		X	X	
THE SECRET SEVEN					
Suppress/alter output	X		X	X	X
Alter master files	X		X	X	X
Introduce deliberate bugs	X		X	X	
Sabotage files/ output	X	X	X	X	X
Partial posting	X		X	X	
Theft of output	X				
Intercycle file tampering	X		X		X

Donn Parker (1977) sets forward a set of security principles that can be used to evaluate various alternative safeguards.

1. "Risk reduction. Each safeguard proposed must be evaluated on the basis of its effectiveness in reducing the risk of an identified threat.

2. Cost of degradation of performance. Each proposed safeguard must be evaluated on the basis of the cost that would be involved to implement, use, and maintain it. Also the degradation of performance of people or functions that are constrained by the safeguards must be considered.

3. Absence of reliance on design secrecy. A well-known principle in cryptography is to design a coding method assuming that the enemy knows as much about the method as the designer and putting all trust only in the keys to the code. The same holds true for any kind of security measure. However, this does not mean that the security methods must be unnecessarily exposed.

4. Least privilege. This principle is also known as the need-to-know. The idea is that the people who work in areas where safeguards are installed should know only as much as is necessary about the safeguards and assets being protected to carry out their jobs effectively.

5. Compartmentalisation. Just as in the safe design of the hull of a ship, each safeguard in a computer center should be designed so that if it is compromised, the loss will be limited to the immediate area without weakening or compromising other areas or functions and thus exposing them to loss as well.

6. Isolation. Good security requires the isolation of sensitive functions. For example, work areas should be laid out so that workers in one sensitive area do not have to walk through other sensitive areas to get to their work stations.

7. Completeness, consistency, and reliability. A safeguard should be complete and consistent with respect to its specifications, and it should function reliably with a minimum of maintenance and human intervention or extraordinary control. The security in a computer center should be complete and consistent to avoid both weaknesses and excessive controls. Computer security is a chain as weak as its weakest link.

8. Instrumentation and threat monitoring. Each safeguard should be instrumented so that attempts to violate it are recorded and brought to the attention of a responsible person.

9. Personnel acceptance and tolerance. For assurance that a safeguard will function effectively, the people who are constrained by it and the people who make it work must accept the need for and purpose of the safeguard and tolerate the constraints it imposes.

10. Sustainability. Safeguards must function effectively, not only when they are first installed but over the entire length of their periods of service. The worst weakness is the safeguard being trusted but no longer functioning.

11. Auditability. Every safeguard must be testable so that an auditor can test it and ensure that it is functioning properly in compliance with specifications and standards.

12. Legal and ethical considerations. Safeguards must comply with the law and must not impose unfair constraints on people. For example, management has a responsibility not to assign a position of trust that exceeds an employee's limit of temptation.

13. Mutual suspicion. Each employee performing a sensitive task must assume he is in a hostile environment. The easiest way to compromise a computer system is to con an EDP employee into doing a favour."

Parker also sets out some of the safeguards found in well-run computer centres (1977).

> "Physical security: Location of the computer center in a low crime area relatively free from sources of natural disasters such as flooding and fire, absence of signs indicating the location of the computer center, protected telephone and power lines, a protected air-conditioning system, positive access control of people entering and leaving sensitive areas, mandatory color-coded badges worn visibly by all employees, adequate smoke and fire detection equipment, fire suppression equipment, adequate water drains and equipment covers to protect from water damage, and backup electrical power.
>
> Procedural and operational security: Separation of responsibility of people in sensitive jobs, dual control over sensitive functions where separation is not practical, periodic briefings and other methods to increase the sensitivity of personnel to the need for security, remote storage of backup supplies and copies of important data files and programs with their operating instructions, control and routine checking of operational logs and exception reports produced automatically by the computer, prohibiting computer programmers from entering the computer room except for emergencies, formal software development methods including independent quality assurance testing of all software, safe disposal of discarded computer output, effective magnetic tape and disk library controls, adequate documentation of security procedures including a disaster recovery plan.
>
> Internal computer security: The operating system must have many characteristics for security and integrity, including adequate authorization for access to the system by users, isolation of user programs and data in the system, passwords used to identify users and their data files, cryptographic capabilities, adequate restart and recovery capability, a threat monitoring and exception reporting capability, and features that reduce the amount of real-time reliance on people."

Mair, Wood and Davis ("Computer Control and Audit" Institute of Internal Auditors 1978)

IPF (Information Processing Function) Control Evaluation Table
Application Control Evaluation Table
Systems Development Evaluation Table
Advanced Systems Evaluation Table
Computer Abuse Evaluation Table

These tables are designed to show firstly the effectiveness of controls in preventing the cause of exposure (top row) and secondly and likelihood that the existence of such a cause of exposure will in fact cause an exposure. Below is shown the computer Abuse Control Evaluation Table which shows, for instance, that 'Dual Access' is ineffective in preventing malicious destruction but reliably controls embezzlement, whereas 'Physical Access Security' reliably controls malicious destruction but is ineffective in preventing embezzlement. The Table also shows that embezzlement is very likely to cause erroneous record keeping but only 'may' cause business interruption.

TABLE 8.7

COMPUTER ABUSE CONTROL EVALUATION TABLE

		OBJECT					TOOL		SYMBOL	ENVIRONMENT				
PREVENTION CONTROLS	REFERENCE	SERVICES THEFT	INFORMATION THEFT	HARDWARE THEFT	MALICIOUS DESTRUCTION	MISCHIEVOUS DESTRUCTION	DESIGN ACT	IMPLEMENT ACT	FRAUD	EMBEZZELMENT	FRAUD	INVASION OF PRIVACY	DESTRUCTION OF MEDIA	UNCORRECTABLE ERRORS
Personnel screening		1	1	1	1	1	1	1	1	1	1		1	1
Definition of duties		1	1	1			1	1		2		2	2	
Segregation of duties		1	1	1			2	2		2		2	2	
Dual access			2							3		2	3	
Professional ethics		1	1	1			1	1	1		1	1		1
Licensing														1
System design controls (a)			1							2	2	2		3
Physical access security		3	2	3	3	3	3	3				2	3	
Electronic access security		2	2		2	2	2	2		2	1	2	2	
Fear of detection		2	2	2			2	2	1	2	2	1	2	2
DETECTION CONTROLS														
External controls			1					2	2		2	2		2
Application controls (a)			2							3	2	2		3
Physical detection		2	2	2	2	1	1	2				1		
Bait records		2	3			1	1	1		1	1		2	
Auditing		2	1	3			1	2	1	2	2		2	3
CORRECTION CONTROLS														
External controls			1				1	2	2		2	2		
Legal actions		2	2	2		2		2		2	2	2	1	
Application controls (a)														3
Contingency plans				1	2	2							2	
Backup and recovery			3	2	3	3							3	
Discharge personnel		3	3				3		3	3		3		
Fidelity insurance		3	3	3	2	2	1	1	1	3	2		2	
			2							3	2			3
											2			
			2	2	3	2				1	1		2	
			2						2					2
			2					2	3	3	3	1		
									2			2		1
		2	1				2						3	2
			3	3	3	3					3			
			2					1						2

RELIANCE ON CONTROLS
3 — Reliably controls applicable cause
2 — Controls cause but should be accompanied by additional controls
1 — Useful but not especially effective
Blank — No significant contribution

EXPOSURES
Erroneous record keeping
Unacceptable accounting
Business interruption
Erroneous management decisions
Fraud
Statutory sanctions
Excessive costs/deficient revenues
Loss or destruction of assets
Competitive disadvantage

IMPACT OF CAUSES
3 — Very likely to occur
2 — Likely to occur
1 — May occur
Blank — Generally little effect

(a) Refer to detailed controls on applicable control evaluation table

Warning: Reliance and impact relationships must be tailored to individual circumstances.
© Touche Ross & Co. Permission expressly granted for reproduction not for sale.

The SAC (1977) report noted:

"Despite a growing awareness of the potential for loss, most top executives interviewed by SRI seemed confident that actual losses are minimal. Yet while some of them maintained that they have not experienced losses related to data processing, they simultaneously admitted that they had no formal procedures to identify and report incidents of this sort. In fact, no organisation contacted during the study felt it had a satisfactory method of measuring overall loss or loss potential".

Also -
"SRI believes that inadequate attention is being given to the importance of internal controls in developing computer-based information systems and in establishing data processing operations. This conclusion applies not only to individual organisations, but to the data processing industry in general. The reason is that each stage in the evolution of EDP systems brings new control problems which require new solutions".

The conclusions of the SAC report are an interesting indication of the current 'state of the art' in the EDP environment.

THE CONCLUSIONS
IN BRIEF "The results of this study show that, although data processing systems and internal audit techniques have been evolving, there has been little coordination between the two disciplines. From the standpoint of those managing the EDP facility, the internal auditors' mandate and their scope of activities are not clear. At the same time, internal auditors are faced with the task of investigating an environment in which most of them have only limited experience, knowledge, and tools. Compounding these conditions is the fact that top management in many organizations has not been sufficiently informed to give adequate attention to the potential repercussions of inadequate EDP audit and control procedures.

In addition to the above general findings, eight specific conclusions were drawn from the results of the study:

1. The primary responsibility for overall internal control resides with top management, while the operational responsibility for the accuracy and completeness of computer-basedinformation systems should reside with users.

2. There is a need for improved controls because inadequate attention has been given to the importance of internal controls in the data processing environment.

3. Internal auditors must participate in the system development process to ensure that appropriate audit and control features are designed into new computer-based information systems.

4. Verification of controls must occur both before and after installation of computer-based information systems.

5. As a result of the growth in complexity and use of computer-based information systems, needs exist for greater internal audit involvement relative to auditing in the data processing environment.

6. An important need exists for EDP audit staff development because few internal audit staffs have enough data processing knowledge and experience to audit effectively in the data processing environment.

7. Few current EDP audit tools and techniques are adequate to the needs of the EDP auditors as they approach the task of verifying the accuracy and completeness of data processing activities and results. New tools and techniques are needed.

8. Many organizations are not adequately evaluating their audit and control functions in the data processing environment. Top management should initiate a periodic assessment of its audit and control programs."

9. DETECTION

In relation to computer abuse, this is the least systematically covered area. There is no one technique or system of techniques designed to uncover computer abuse. As things stand currently the emphasis when combatting computer abuse must be in preventative measures i.e. control.

The public and even management may be forgiven for assuming that fraud detection is part of the role of the auditor - they are wrong. The external auditors expressly deny any responsibility for fraud detection unless the extent of the fraud would be such as to materially alter the ability of the financial statements to present a fair and true picture. Thus something in the realm of an Equity Funding scheme becomes a responsibility for the auditor to detect, but as one American auditor has stated ...

> "The sort of frauds that have taken place, while the amounts involved might seem high, have not been what in our parlance we term material; that is, they have not had a major impact on the fairness of a financial statement." (New Yorker 22.8.1977)

Thus external auditors are primarily concerned to establish the reliability of the financial data within certain parameters of certainty e.g. 95%. Accordingly they have an approach to assessing this reliability based upon techniques to:

(i) assess the overall system of control;

(ii) test compliance with those controls; and

(iii) test samples of data in order to substantiate its reliability within forecast perameters.

In practice this means that the more the quality of the control system can be assured by compliance testing, the less requirement there will be for substantive testing.

Even these data verification tasks have been rendered more difficult by the computer. Traditionally the auditor has relied on being able to check manual records, controls and transactions and this changed very little with the introduction of batch processing on the computer when it was little more than a gigantic adding machine whose function could be verified by comparing input and output control totals.

Now, however the DP environment is changing rapidly with the advent of

(i) real time remote entry terminals;
(ii) data-base systems or similar where one transaction may update several related functions;
(iii) replacement of 'hard-copy' audit trails by transaction logs on mag tape and by on-line data bases for master data file interrogation.

Thus, from the point of view of gaining assurance on controls the auditor has to increasingly move his techniques 'into' the system, yet -

"SRI has identified and documented 28 tools and techniques used by internal auditors for auditing computer-based information systems, computer service center operation, and the systems development process. However, most the these have been used as after-the-fact checks, rather than being built into the system. Few are adequate to the current or future needs of the EDP auditor. Unless greater emphasis is placed upon development of such tools and techniques, the gap between the sophistication of the computer-based information systems and the capability to audit them will continue to widen.

At present, the most frequently used tool or technique is generalized audit software, a tool most suitable for verification of data. (cf. respondents to the primary U.S. Mail Survey. 33% reported employing this approach). Use of tools and techniques designed to evaluate and verify controls is reported less often. (The SAC Report 1977)

In summary then,we have an audit profession who are primarily concerned with the overall picture of a company's affairs within the framework of statistical levels of confidence, that profession is not concerned with the detection of "immaterial" levels of fraudulent activity. As a result the auditor's approach and the techniques he uses are designed for purposes other than detection.

Its not that computer fraud is undetectable, it's more that no one is sufficiently aware of a responsibility for its detection to design the requisite approach and techniques. Prevention is the responsibility of management -spurred on by auditors and others - and it is reasonably economic. On the other hand detection, at its current stage of development, is likely to be costly with unknown or severely limited potential for economic return.

Objections to this argument may come from two quarters. First that the internal auditor must have a responsibility for fraud detection, and second that if an auditor finds the quality of controls sufficiently poor such that the potential for abuse is high, then surely he must have a responsibility to detect such abuse.

Quite apart from the fact that the internal auditor has essentially the same tools at his disposal as does the external auditor - and they are not designed for detection - the internal auditor is primarily not a detective but a "high level element of the total internal control of an organization". As such his work in instituting checking and improving controls is frequently grounds for a lessening of the substantive testing by the external auditor.

"The usual scope of examination by internal auditors concentrates on compliance audits and puts little emphasis on substantive procedures."

In the instance of poor quality of controls, the auditor has an obligation to increase the amount of substantive testing to the point where he attains a satisfactory level of assurance as to the reliability of the financial data. He may be forced to qualify the accounts, he may perhaps uncover fraud, but once again he has no responsibility to satisfy himself or management that fraud has not occurred.

Auditors have been quoted as saying that two things must occur for fraud to be detected - the auditor must get lucky and the perpetrator must be clumsy.

Auditors go looking for poor controls which endanger the financial system, for individual gross errors which could distort the figures and for systematic repetitive errors which can also distort but which are susceptible to detection following application of the laws of probability. They frequently uncover clumsy schemes of fraud and stand a better chance of doing so when the audit trail is visible. In modern computer environments the ability of many auditors to carry out their historical responsibilities has been called into question, the usefulness of many of the tools available may be doubted, and the chances of detecting the more sophisticated varieties of computer fraud must be slim indeed.

Brandt Allen, 1977
"Of the more than 50 examples I have studied fewer than half were first detected by auditors or internal controls. A great many of these cases involved very simple schemes that could have continued to be successful for much longer, or for indefinite periods of time, had the perpetrator been a little more clever."

Following the entry of fraudulent transactions into the U.S. Internal Revenue Service and independent security consultant Lindsay Baird stated,

> "They (the I.R.S.) wanted to find a way of patching up the system to prevent similar incidents, of course, but I told them that it couldn't be done - that, among other things, the system had not been designed with auditability in mind."

Donn Parker

> "EDP auditing is becoming an important security function. Safety in using EDP will depend principally on this function for the next few years until more powerful technological solutions are achieved. EDP audit techniques and adaptions of traditional security practices can do no more than contain the problem today. They can't protect society from computer abuse perpetrated by the computer systems programmers, computer operators, and maintenance engineers. No practical way has been devised to audit the work of these people sufficiently because of the increasing complexity of computer systems and the lack of standards, discipline, and structured practices in their design and construction. A large computer system exceeds in complexity man's capability of demonstrating its integrity over periods of time - the assurance that it conforms to a complete, adequate, and consistent set of specifications, and contains no compromising parts beyond those required in the specifications. It is anticipated that this basic requirement will be achieved when the design, development, and construction methodologies mature from cottage crafts to technologically sound disciplines, and when security principles become an integral part of system design from the start. This will require another generation of computers after these steps become common practice. We can anticipate that these new systems and equally secure environments in which to put them will surface in the early 1980s, assuming that forthcoming technological advances in system types and use do not preclude the security concepts and methodologies now being developed.
>
> It must be recognized that the time could come when new applications of computers and new computer system designs would be limited by the lack of safety in their use. It is essential to monitor and report on computer abuse in order to reduce the danger of applied technology advancing beyond this point without our knowing it."

I am not setting out to criticize the role of the auditor since he has been caught by rapid technological advance and by what might be termed the blind irresponsibility of many computer manufacturers, system designers and computer users in putting together or operating systems that invite abuse and cripple the role of the auditor.

It is important to remember that the auditor is primarily an extension of the computer abuse prevention part of the spectrum, his principal task relates to the assessment of the controls within an organisation since they have such an important effect on his conclusions regarding the fairness of financial statements. Nevertheless I have chosen to include discussion of audit techniques under the Detection Section since no other techniques have been written about detection to my knowledge, and since, although they may not specifically have been designed for that purpose, they may be of use in the detection of computer abuse.

The following then is an attempt to give a brief outline of the attributes and usefulness of EDP audit techniques, nearly all of which have been taken initially from the SAC report. Shown below is the report's index which I have followed in presenting my analysis. Additional techniques have been noted.

DATA PROCESSING AUDIT TOOLS AND TECHNIQUES

Audit Planning and Management
  Audit Area Selection
  Simulation / Modeling
  Scoring
  Multisite Audit Software
  Competency Center
Testing Computer Application
Program Controls
  Test Data Method
  Base Case System Evaluation
  Parallel Operation
  Integrated Test Facility
  Parallel Simulation
Selection and Monitoring of
Data Processing Transactions
  Transaction Selection
  Embedded Audit Data Collection
  Extended Records
Verification
  Generalized Audit Software
  Terminal Audit Software
  Special-Purpose Audit Programs
Analysis of Computer Programs
  Snapshot
  Manual Tracing and Mapping
  Computer-Aided Tracing and Mapping
  Control Flowcharting
Computer Service Center
  Job Accounting Data Analysis
  Audit Guide
  Disaster Testing
Application System Development
  Postinstallation Audit
  Control Guidelines for Use During System Development
  System Development Life Cycle
  System Acceptance and Control Group
  Code Comparison

The report also includes the result of a survey on the usage of such techniques.

A. Use of EDP Audit Tools and Techniques

Which of the following tools and techniques are used in auditing EDP application systems in your organization?

EDP Audit Tool/Technique	Percentage Used in Auditing Developments and Modifications	Percentage Used in Auditing Production Systems
Generalized audit software	12.5%	32.6%
Manual tracing and mapping routines	22.8	31.2
Test data method (e.g., test-decking)	27.1	26.6
Parallel operation	32.2	23.1
Tagged transactions (flagging transactions in "live" operations for later review)	12.0	20.9
Snapshot (picture-taking of selected transactions through the flow of transactions	10.0	18.4
Systems performance monitoring and analysis (e.g., SMF, SCERT)	8.2	15.8
Program source code comparison	9.6	14.5
Control flowcharting	8.3	9.0
Program object code comparison	4.7	8.9
Integrated test facility (mini-or dummy company)	4.2	5.0
Modeling (simulation)	9.5	7.6
Automatic tracing and mapping routines (analysis of source language and logic to determine if any program segments are not being utilized)	3.6	3.9
Other	6.5	10.5

B. Techniques to Test Computer Application Programme Controls

Practices whose primary concern is to check compliance to organization policies and procedures and the controls designed into applications to ensure compliance to these policies and procedures.

Test Data Method

Base Case System Evaluation

Parallel operation

Integrated Test Facility

Parallel Simulation

TEST DECKS

Method: Preparation of predetermined input data that are processed under the auditor's control by the client's processing system. Output is compared to the auditor's predicted output.

Purpose: Essentially programme verification
Particularly suited for testing and verification of computer application systems that are undergoing minimum change

Advantages:
Little technical knowledge required by auditor
More effective if the variety of possible conditions is limited
Auditors forced to become familiar with the logic of the overall system
Particularly suited to batch systems

Disadvantages:
No guarantee that the programme tested is the one normally always in use.
Problem with design of comprehensive test data.
- "test-data-generator" software may help to overcome this problem.

Time consuming if extensive tests are performed.
Tests to be limited to specific processing functions, computations, or controls, rather than to comprehensive testing of entire applications.
Requires reversal entries if run against live files.

BASE CASE

Method: Preparation of a standardised body of data, designed to check all situations and which can then be applied to the testing of changes.

Purpose: Similar to Test Decks but involves more people in analysis of requirements.

Advantages:
High degree of user involvement
Once BC prepared, subsequent system test are easier.

Disadvantages:
Expensive initial preparation.
Great deal of time input required by users, auditors, etc.
Cannot provide evidence concerning data file content and integrity, procedure compliance or input accuracy and thoroughness.
Requires reversal entries if run against live files.

PARALLEL OPERATION

Method: Run old and new systems "in parallel", compare results and analyse causes of discrepancies.

Purpose: To verify accuracy of replacement or revised application system programmes.

Advantages:

Builds user confidence in new systems

Disadvantages:

Costly
May be very difficult to co-ordinate running two systems in parallel
Does not say anything about controls built into programmes.

INTEGRATED TEST FACILITY

Method: Auditor initializes a dummy file and processes data through the regular processing system against the new file. Test data is thus "integrated" into the regular system of processing.

Purpose: A programme verification technique. Enables the auditor to randomly monitor process systems throughout the year, thereby increasing the probability that the process tested is the one generally used.

Advantages:

Tests operation under 'normal' conditions
No special processing requirements
Can have unscheduled checks on the system

Disadvantages:

A method must be designed to separate results of test data from 'real' data
- journal entry
- modify programmes
- create separate unit, e.g. division, company, department.

There is still a danger of'pollution' of real data,
Time consuming
Provides limited evidence of the accuracy or completeness of input data or masterfile data
Needs to be built into the original design of software

PARALLEL SIMULATION

Method: The processing of "live" data through 'audit' programmes which resemble the logic of the application programmes but which only test the features of the system which require to be audited, results can then be compared with results from operating system.

Purpose: Allows verification of computer applications for correct
- input data validation and control procedures
- computations and processing logic
- masterfile updating logic
- controls and balancing procedures

Advantages:

Enable more thorough validation than with a data sampling technique
Audit checks can be performed at any time depending on availability of the computer

Disadvantages:

Time and cost necessary to design and develop parallel simulation programmes (use of GAS can reduce these expenditures).
"Is virtually auditing around the computer with the computer".
Requires detailed knowledge of the application programme,
- high degree of training on part of auditor.

Continuing expense in keeping up with changes in application programmes.
Limited evidence is provided on the accuracy or completeness of input data or computer files.

C. Selection and Monitoring of Data Processing Transactions

Practices designed to check compliance of data processed by computer applications to organizational policies and procedures. A prime purpose is to verify the adequacy of internal controls.

Transaction Section

Embedded Audit Data Collection

Extended Records

TRANSACTION SELECTION

Method: Auditor uses software to monitor select and report on particular transactions according to parameters determined by him.

Purpose: Allows auditor to monitor activity, error rates etc of transactions which are of a significant nature.

Advantages:

Useful aid to identification of problem areas, and planning audit work.

Disadvantages:

Only references can be made about how well sample transactions represent the remaining population.
Need to put transactions through a second time for the transaction selection programme.
Not a good technique for on-line systems.
Provides no information regarding the computer application system processing logic, or data file accuracy, integrity, or completeness.

EMBEDDED AUDIT DATA COLLECTION

Method: Insert one or more specially programmed data collection modules into the computer application system. These can then select and record data according to auditor-determined parameters.

Purpose: Collection of audit data, and monitoring of specific transactions for 'cause of concern'.

Advantages:

Operates on line i.e. 'live'.
Comprehensive ability for transaction review.
Allows monitoring on a continual basis.
Minimal additional computer running time.

Disadvantages:

Best suited for inclusion at time of writing the application programme.
Requires higher level of skill on part of internal auditor
Fairly time consuming and costly to develop.

EXTENDED RECORDS

Method: Use of special programme(s) to gather all the significant data that have affected the processing of an individual transaction over a period of time and/or through different programming modules.

Purpose: To provide a comprehensive audit trail.

Advantages: Enables simplified retrievals of full transaction data from one computer record.
Most suitable for high risk financial situations: - cash or valuable, merchandisable inventory.
Increases control, because it is more difficult to conceal processing exceptions.
Consolidates records from several time periods.

Disadvantages:
Must be built into computer application systems.
Very costly - modifying programmes, additional processing time, additional storage area (- 5% cost of Application System).
Largely unnecessary with online data base systems.

D. Verification

Practices used primarily for substantive testing of data

Generalized Audit Software

Terminal Audit Software

Special Purpose Audit Programmes

GENERALIZED AUDIT SOFTWARE

Method: Set of computer programmes that have the capability to process computer data files under the control of input parameters supplied by the auditor - Packages available generally provide:-

- footing, cross footing, and balancing data;
- selecting and presenting detailed data from a file;
- performing various logical operations on data;
- stratifying data;
- statistical sampling and extracting information;
- formatting reports and preparing confirmation statements;
- screening specific data elements on a file (e.g. duplicate, missing information);
- comparing same file over 2 time periods or different files with same information for same time period.

Purpose: Verification:- to test, examine, and balance automated records

Advantages: Minimal training required of auditor.
Flexible or quickly prepared.
Most common auditing technique .'. wide expertise available.
Moderate cost.

Disadvantages: Present nominal applicability to on-line systems.

TERMINAL AUDIT SOFTWARE

Variation:- accesses, extracts, manipulates, and displays data from on-line data basis using remote terminal inquiry commands.

SPECIAL-PURPOSE AUDIT PROGRAMMES

Specifically tailored programmes.

"Generalized Audit Packages are only an extension of manual auditing techniques and procedures. At best they can provide partial assurances about the quality of information on file".

E. Analysis of Computer Programmes

Practices for evaluating computer programmes to ascertain they are functioning as specified and in accordance with organizational policies and procedures.

Snapshot

Manual Tracing and Mapping

Computer-Aided Tracing and Mapping

Control Flowcharting

* Auditing Load Libraries

* Programme Code Checking

* Not quoted in SAC study

SNAPSHOT

(A variation of Tagging and Tracing)

Method: Marking or tagging client input data such that relevant information is displayed at key parts in the processing system. Snapshot - prints out (part of) memory at pre-selected points in the processing of a transaction.

Purpose: To create a data 'audit trail' through the computer processing stage.

Advantages:

Use of actual data under 'live' circumstances.
Useful in conjunction with ITF.

Disadvantages:

Extreme increases to processing times.
No guarantee that all logic paths are traversed or that an indication of their existence will be provided.
(normally) limited to use in new computer applications.
Requires highly skilled analysis to set up.

TRACING

Method: (Normally) Use trace option available in several of the high level computer languages, it involves a special compilation of source code. On activation it provides a listing of the programme statements that were executed during the processing of the (either) specific or selected group of transactions in question.

Purpose: To show how transactions are processed through computer programme.

Advantages: Particularly useful for complex debugging.

Disadvantages:

Costly both in terms of computer time and manpower analysis time
Calls for intimate knowledge of the computer application programme on the part of the user.

MAPPING

Method. Use of available software measurement tools to report on any or all of:
- a list of any programme segments not executed;
- a list of the steps consuming the most CPU time;
- a list of the source programme showing the total number of times that each statement was executed.

Purpose: To assess the overall efficiency of the programme, to isolate unexecuted code which has a security risk.

Advantages:
Useful for improving efficiency of computer system.
Pinpoints major security problem area-unused code.
Assesses usefulness of testing and debugging routines.

Disadvantages:
Require internal auditor to comprehend the computer programme logic.
Do not prove that the programme performs in accordance with the intent of the systems analyst, do not prove that execution was in the proper sequence. Takes a long time to develop the test data and execute the tests .
Preprocessing, performed by some mapping techniques may alter source code so as to camouflage malicious code. Some versions may require an unreasonable degree of expertise for interpretation of output.

CONCURRENT PROCESSING

A variation on mapping involving continuous monitoring by a software 'supervisor'. Designed specifically to detect exception or unusual conditions and to record information about the initiating transaction.

CONTROL FLOWCHARTING

Method: Use flowcharts to graphically portray the identification and interrelationships of controls.

Purpose: To define all the controls relating to a system in the total business context of that system.

Advantages: Useful method to identify lack of control in key areas
Useful for training and communication.
Most useful when applied to the development of new systems.

Disadvantages:
Requires particular skills on the part of the auditor.

AUDITING LOAD LIBRARIES

Method: Comparison of load library (machine language programme library) directory to pick up additions, deletions and changes.

Purpose: To check all programme alterations to ensure their validity.

Advantages:

Easily performed by simple computer programme.
Compares object code and not source code.

Disadvantages:

Will not detect changes which do not alter the length of the directory.
In a changing environment may require a great deal of analysis to determine the validity of all programme modifications.
Assumes you are checking the load library that is normally in use.

PROGRAMME CODE CHECKING

Method: Analyse in detail the process code for validity, controls etc.

Purpose: To ensure programme compliance with all audit objectives.

Advantages:

Thorough examination of programme.
May be the only valid technique where something is suspect.

Disadvantages:

Virtually impossible with a large complex system to examine every line of process code.
Requires very sophisticated expertise on the part of the auditor.
Very cumbersome and time consuming.

10. BIBLIOGRAPHY

Adams, D.L., "COMBI (Cobol Missed Branch Indicator) An Audit Tool," EDPACS, (April 1975)

" " "Audit Review of Program Code-1", EDPACS (August 1975)

" " "SMF - An Untapped Audit Resource", EDPACS (September 1974)

" " "Audit Software - DYL -250 and DYL-260", EDPACS (July 1974)

" " "Audit Software Requirements", EDPACS (November 1973)

" " "A Survey of Test Data Generators", EDPACS (April 1973) and J.F. Mullarkey, "A Survey of Audit Software", *Journal of Accountancy* (September 1972)

AICPA, Computer Auditing Subcommittee's Auditing Advanced EDP Systems Task Force, "Advanced EDP Systems and the Auditor's Concern", *Journal of Accountancy* (January 1975)

" Auditing Standards Executive Committee "The Effects of EDP on the Auditor's Study and Evaluation of Internal Control", *Statement on Auditing Standards No.3* (December 1974)

" Committee on Auditing Procedure, "Modification of Auditing Standards and Procedures," *Statement on Auditing Standards No. 1* (November 1973)

Bjork, L.A., "Generalized Audit Trail Requirements and Concepts for Data Base Application", *IBM Systems Journal No. 3* (1975)

Boutell, W.S., ed., *Contemporary Auditing* (Dickenson, 1970)

" "Auditing Through the Computer", *Journal of Accountancy* (November 1965) pp.41-47

" *Auditing With the Computer* (University of California Press, 1965)

Brandt, Allen "The Big Computer Frauds: Lessons for CPAS" *The Journal of Accountancy, May 1977*

" " The Embezzlers Guide to the Computer" *Harvard Business Review,* July-August 1975

Bryden,W.A., "A Case Study in Computer Auditing of a Small Company", *Journal of Accountancy* (March 1976)

Burke, E.L., "Synthesis of a Software Security System" (MITRE Corporation, September 1974)

Cash, J.I., Bailey, Whinston, "A Survey of Techniques for Auditing EDP - Based Accounting Information Systems", *The Accounting Review* (Oct.1977)

Cash, J.L., W.D.Haseman and A.B.Whinston, "Security for the GPLAN System", *Information Systems* (October 1976)

Cerullo, M.J., "Procedures for Auditing Around EDP Service Bureaus", *Florida Certified Public Accountant* (July 1974), pp.11-14

Chambers,A.D., "Audit Test Packs and Computer Audit Programs,"*The Computer Journal,* No.2 (1975)

Christopher, D.W., and J.R.Keith, "Case Study of a Computer Audit Program: An Application of a Computer to the Audit of the Recording Function for Fixed Assets in a Heavy Industry Company", *Price Waterhouse Review* (Spring 1968)

" and J. A. Richards, "Case Study of a Computer Audit Program", *Journal of Accountancy, v.123* (April 1967) pp.69-73

(CICA) "Computer Control Guidelines" and "Computer Audit Guidelines" *Toronto: CICA* 1970 and 1975

Cloyd,H.M., "Continuous Auditing - What is its Future?" *National Public Accountant* (January 1971)

" "Auditing Through the Computer", *National Public Accountant* (January 1967) pp.20-22

Crabtree,M.G. and A. Oakley, "Interrogation Kit - A Description of Generalized Audit Program, ASK 260", *Accountancy* (Eng.) (November 1969) pp.820-827

Davis,G., *Auditing and EDP* (AICPA,1968)

Davis,W.W. and D.R.Wood, "Computer Control and Audit", *Touche Ross Tempo,* v.18, (Autumn 1972) pp.9-20

Doherty, H.S. and J.L.Sorenson, "Use of Computers in Auditing", *Arthur Joung Journal* (Special Issue, 1970)
EDPACS, "Auditing a Data Base System" (March 1975)
Fine,L.H. "Data Base: The Role of the Auditor", *Data Systems,* June 1976
Gould,K. "Computer Performance Measurement Techniques", First Annual EDP Auditors Conference (1973)
Haskins & Sells & Co., "Auditape", *H & S Reports* (Autumn 1966), pp.4-7
Horwitz, G.B., "Needed: A Computer Audit Philosophy", *Journal of Accountancy* (April 1976)
Hulme, K.G. and Aitken, M.E. "A Normative Approach to Internal Control Evaluation of On-Line,Real-Time Systems", *The Chartered Accountant in Australia* - July 1976
Jancura,E.G., "Technical Proficiency for Auditing Computer Processed Accounting Records", *Journal of Accountancy* (October 1975)
" and A.H.Bergen, *Computers: Auditing and Control,* (Auerbach,1973)
" *Audit & Control of Computer Systems* (Petrocelli, 1974)
Johnson, E.C. "Computer as an Audit Tool", *California CPA Quarterly* (June 1974)
Kiefer, G. H., "Systems Auditing with Test Decks", *Management Accounting* (June 1972) pp.14-18
Kunkel,J.G., "Continuous Auditing by Exception", *Management Accounting* (July 1974)
Leishman, R.O., "Computer as an Auditing Tool", *Internal Auditor* (January-February 1971) pp.22-27
Li, D.H., "Audit-Aid: Generalized Computer Audit Program as an Instructional Device", THE ACCOUNTING REVIEW (October 1970)pp.774-778
" *Accounting-Computers-Management Information Systems* (McGraw-Hill,1968)
Liebholz & Wilson, "User's Guide to Computer Crime"
Loebbecke, J.K., "Internal Control Evaluation: How the Computer Can Help", *Journal of Accountancy* (August 1975)
Mair,W.C., K.W.Davis and D.R.Wood, *Computer Control and Audit,* (Institute of Internal Auditors, 1976)
" " "PARALLEL STIMULATION - A Technique for Effective Verification of Computer Programs", *EDPACS* (April 1975)
" *New Techniques in Computer Program Verification* (Touche,Ross & Co., Inc., 1971)
Martin, J., *Security,Accuracy and Privacy in Computer Systems* (Prentice-Hall, 1973)
McCosh,A.M., Earl M.J., "The Audit of Computer Programs" *The Accountant's Magazine,* July 1976
McRae.,T.W., "Need We Audit The Program?" *Accountant* (Eng.), (June,1966), pp.806-807
Meikle,G.R. and J.B. Gambles,"Auditape for Management and the Auditor", *Accountancy* (Eng) (July 1969) pp.493-500; (August 1969) pp.583-591
Merich, L.C., "Data Processing Auditing: Using a Computer-Assisted Approach", *California CPA Quarterly* (December 1973) pp.36-37
Merrill,W.W., "Auditing with the Computer - Basic Principles", *Massachusetts CPA Review* (January February 1972), pp.28,31.
Milko, E.M., "Auditing: Through the Computer or Around"? *Management Accounting* (August 1970)
Moore, M.R. and R.H.Yocom, "The AY Audit/Management System: An Information Tool for Auditors and Managers", *Arthur Young Journal* (Special Issue, 1970)
Moore, R. "Computer Generated Documentation", *Journal of Accountancy* (June 1975)
Parker, D.B., *Crime by Computer* (Scribner's Sons, 1976)
Perry, W.E., "Using SMF as an Audit Tool - Accounting Information", EDPACS (January 1975)

Perry,W.E., "Using SMF as an Audit Tool-Performance", EDPACS (December 1975)
" "Using SMF as an Audit Tool-Security", EDPACS (January 1976)
" and D.L.Adams, "SMF - An Untapped Audit Resource", EDPACS(September 1974)
" "Concurrent EDP Auditing: An Implementation Approach", EDPACS (February 1974)
" "Concurrent EDP Auditing: An Early Warning Scheme", EDPACS (January 1974
" "Try ITF, You'll like ITF", EDPACS (December 1973)
" SNAPSHOT - A Technique for Tagging and Tracing Transactions", EDPACS (March 1974)
Piket,T.P., "AUDIT Retrieval - the New Frontier for Auditors", *U.S. Army Audit Agency Pamphlet, No.350-2* (June 1974) pp.16-22
Poplawski, E.J., "Auditing Around or Through the Computer", *Magazine of Bank Administration* (November 1974) pp.22-24
Porter, W.T., *EDP Controls and Auditing* (Wadsworth, 1974)
" "Generalized Computer Audit Programs", *Journal of Accountancy* January 1969)
Raffensperger, O.E., "Computer as an Audit Tool", *Internal Auditor* (November December 1973) pp.72-74
Reid, G.F. and J. Demeak, "EDP Audit Implementation with General Purpose Software", *Journal of Accountancy* (July 1971), pp.35-46
Reneau, J. H., "Auditing in a Data Base Environment" *The Journal of Accountancy* Dec.1977
Rittersbach and Harlan, "Auditing Advanced Systems", *Journal of Accountancy* (June 1974)
(SAC) "Systems Auditability and Control" - 3 vols. *Institute of Internal Auditors,* 1977
Sady, M. and R.J. Joyce, "Generalized Computer Programs - Are They Worth the Effort"? *GAO Review* (Fall 1970), pp.48-54
Schaller, C.A., "Auditing and Job Accounting Data", *Journal of Accountancy* May 1976)
Schick, C.W. and V.J.Perrill, "Using the Computer as an Auditing Tool", *New York Certified Public Accountant* (January 1969), pp.57-60
Schroeder, W.J., "Memo on Installing a Data Base System", *Journal of Accountancy* (February 1974) pp.81-82
Sethna, R., "A Blueprint for Generalized Computer Audit Systems", *C.A. Magazine,* August 1976
Shell, R. C., "Audit Control Over Computer Programs", EDPACS (March 1975)
Smith, C.O. and G.F. Jasper,"Using the Computer in Audit Work", *International Accounting* (Eng.) (April-June 1973), pp.8-12
" and G.F.Jasper, "Using the Computer in Audit Work", *Management Accounting* (October 1972) pp.34-38, 42.
" and G.F. Jasper, "Using Computer-Aided Techniques in Financial Audit Work", *GAO Review* (Fall 1971), pp.28-37
" "Useful Techniques for Examining Automated Data Processing Systems", *GAO Review* (Fall,1969) pp.27-35
Spinelli,C.C., "Auditing Accounts Receivable by Computer - A Case History", *Journal of Accountancy* (April 1970) pp.73-78
Stettler, H.F., *Systems Based Independent Audits* (Prentice-Hall, 1974)
Stickler, V.D., "An Appraisal of Flow Charting as an Audit Technique", *Internal Auditor* (July/August 1972)
Stone, R.L., "Security and Integrity Controls in Small Computer Systems", *Journal of Accountancy* (February 1976)
" "Who is Responsible for Computer Fraud"? *Journal of Accountancy* (February 1975)
Studldreher, W.F., "Can Auditors Actually Audit 'through' the Computer"? *U.S. Army Audit Agency Bulletin* (Summer 1969), pp.33-36

Taylor,A.R., "Audit of A.D.P. Systems Using Test Decks and Test Files", *Australian Accountant* (May 1969), pp.206-210

Thibeau, P.B., "Auditape: A Versatile Audit Tool", *GAO Review* (Fall 1970), pp.55-59

Touche, Ross & Co., National Accounting and Auditing Staff *Computer Controls and Audit,* (September 1973).

Wasserman, J., "Selecting a Computer Audit Package", *Journal of Accountancy* (April 1974), pp.30,32,34.

Weber,R. and A.M.Jenkins, "Using DBMS Software as an Audit Tool: The Issue Of Independence", *Journal of Accountancy* (April 1976)

" "Audit Capabilities of Some Data-Base Management Systems", Fifth IIA Conference on Computer, Audit, Control and Security (April 1975)

" "An Audit Perspective of Operating System Security", *Journal of Accountancy* (September 1975)

" and C.R. Litecky, "The Demise of Generalized Audit Software Packages", *Journal of Accountancy* (November 1974)

" "This Business of Database Management and What it Means to the Accountant and Auditor", (University of Minnesota, Graduate School of Business Administration, October 1974)

Weiss, H.L., "The Use of Audit Indication and Integrated Test Facility Techniques", EDPACS (July 1973)

Weissman Clark "Trade Off Consideration in Security System Design" *Data Management,* April 1972

Welke, W.R. and K.G.King "Using the Computer as an Audit Tool", *CPA Journal* (November 1972), pp.930-932

White, D. C., A.R. Whitesell and J. W. Bynum, "Using Test Decks in Financial Audit Work", *GAO Review* (Spring 1972) pp.33-39

Will,H.J., Brussel & Clark, "An Invitation to Help Develop New Audit Software" *C.A.Magazine* May 1977

Will, H.J., "Computer Based Auditing - Parts 1 and 2 *C.A.Magazine* February - March 1972

Wlodarek, R.A., "Using an ADP Information Retrieval System in Auditing an Educational Assistance Program", *GAO Review* (Fall 1970) pp.60-67

Woellner, D.A., "Auditing Through Computers", *Federal Accountant* (Spring 1966) pp.20-29

Wohl,G. and M.D'Angelico, *Computer in Auditing - The Use of Test Data* (Richard D. Irwin Inc., 1966)

Wright,R. G., "Auditing Through the Computer", *Oklahoma CPA* (July 1966) pp.7-14

SECTION 2.

A SELECT BIBLIOGRAPHY OF FURTHER READING ON COMPUTER ABUSE PUBLISHED SINCE 1975 AND AVAILABLE FROM AUSTRALIAN LIBRARIES.

Compiled by: JEAN GOURLAY

AARON, H.R. 'Managing the corporate computer security problem'. *Security Management*, v.21,Nov.,1977.pp.14-17.

ABDULLAH, Mian Mumtaz 'Data control and audit'. *Industrial Accountant*, v.15,Oct./Dec.,1976.pp.231-5.

ADAMS, Donald A. 'Computer fraud goes to the dogs'. *Edpacs*, v.5,Jan.,1978.pp.8-9.

ADAMS, Donald L. 'Audit & Control of TSO-part 1'. *Edpacs*, v.3, March,1976.pp.1-11.

ADAMS, Donald L. 'Computer security hardware devices & services-II'. *Edpacs*, v.5,July,1977.pp.10-16.

ADAMS, Donald L. 'FAIM technical publications - an approach to the review and evulation of EDP'. *Journal of accountancy*, v.140,Sept.,1975.pp.100-3.

ADVANCED SYSTEMS INCORPORATED VIEWERS GUIDE. 'Computer crime, fraud and embezzlement'. 1977.p.15.

'AFIPS offers data security study'. *Electronic news*, v.19, Oct.14, 1974.p.52.

AIKEN, Maxwell E. *Normative audit control for on-line/real-time systems; a feasibility study*. Kensington, Australia, University of New South Wales, 1974.

ALBI, F.J. 'Foiling the computer criminal'. *Banking*, v.70,May, 1978.pp.67-70.

ALEXANDER, T. 'Waiting for the great computer rip-off'. *Fortune*, v.90,July,1974.pp.142-6+.

ALDERMAN, Tom. 'Computer crime'. *Journal of systems management*, v.28,Sept.,1977.pp.32-5.

ALLEN, Brandt. 'Biggest computer frauds:lessons for CPAs'. *Journal of accountancy*, v.143,May,1977.pp.52-62.

ALLEN, B.R. Embezzlement of automation. 12th IEEE Computers Society International Conference on Computers the Next 5 Years. (Digest of papers), San Francisco, Calif., USA, 24-26 Feb.,1976 (New York,USA:IEEE 1976),pp.187-8.

ALLEN, B. 'Embezzler's guide to the computer'. *Harvard Business Review*, July/Aug.,1975.pp.79+.

ANDERSON, G.S. 'Computer manipulation robs our firms of millions of dollars a year'. *Management World*, July,1977.pp.7-10.

Approaches to privacy and security in computer systems;proceedings of a conference held at the National Bureau of Standards, March 4-5,1974. *Washington, National Bureay of Standards*, 1974.

ARMER, Paul. 'Individual:his privacy, self image, and obsolescence'. *Computers and people*, v.24,June 1975.pp.18-23,31.

AUBURN, F.M. 'Computer privacy-a Commonwealth precedent'. *Law & Computer Technology*, v.9, no.2, Sept., 1976. pp.30-43.

AUERHAMMER, Dr. 'Data security means citizens' protection'. *ICA Information*, no.13, May, 1978. pp.5-9.

BAILEY, R. 'Privacy, data protection, security and computers'. *Accountant* v.178, May, 25, 1978. p.707.

BAIRD, Lindsay L. 'Auditing the computer center'. *Risk Management*, v.23, Aug., 1976. pp.50-2, 54-6.

BAIRD, Lindsay L. 'Safeguarding computer software from damage or manipulation'. *Newspaper controller*, v.28, June, 1975. p.10.

BAKER, D.W. 'Top-management fraud' *The Internal Auditor*, Oct. 1976. pp.25+.

BALL, L.D. 'Maintaining security and privacy in educational computer centers: a growing problem'. *AEDS JOURNAL*, v.11, Fall, 1977. pp.6-13.

'Be ready for the computer crooks'. *Rydges*, v.49, Dec. 1976. pp.99-107.

BEATTIE, M. 'Managing security'. *Management Today*, April 1975. pp.34+.

BECKER, H.B. 'Securing distributed systems: gaining by losing control'. *Data Management*, v.16, March 1978. pp.24-6+.

BENTLEY, T.J. 'Auditability and control of computers'. *Management accounting*, v.55, Jan. 1977. pp.13-14.

BEQUAI, A. 'Crooks and computers'. *Trial*, v.12, Aug. 1976. pp.48-9.

BEQUAI, A. 'Legal problems in prosecuting computer crime'. *Security Management*, v.21, July, 1977. pp.26-27.

BERETTA, P. 'Preventing auditing in the sphere of automatic data processing'. *Sist. & Autom.*, v.24, no.180, March 1978. pp189-91.

BERG, John L. 'Federal privacy act countdown - is the private sector ready?' *Infosystems*, v.22, July, 1975. pp25-6.

BERKERY, Michael J. 'Computer control and audit in the public sector', *Governmental finance*, v.6, Aug. 1977. pp.34-40.

BEST, Peter J. 'Unauthorized remote access in an on-line real-time system'. *Australian accountant*, v.45, March, 1975 .pp106-8, 111.

'Big brother computer'. *Economist*, v.262, Jan. 29, 1977. p.27.

'Black magic from the black box'. *Accountant*, v.175. Oct. 7, 1976. p.414.

BOCHE, R.E. 'System software deciphering'. *Comp. & People*, v.23, July, 1974. pp.10-13.

BOCKELMAN, Melvin F. 'Police department's security kept under surveillance', *Infosystems*, v.22, May, 1975. pp.65-6.

BOWERS, D.M. 'One computer protects another'. *Office*, v.86, Aug. 1977. pp.77-8+.

BRANSTAD, D.K. 'Data encryption: now you see it, now you don't', *The EDP Auditor*, Aug. 1977. pp.4-6, 8.

BRIGHT, Herbert S. 'Computational crytography & security'. *Edpacs*, v.5,Sept.,1977.pp.1-8.

BRILL, K.G. 'Planning for good power protection'. *Comp. Decisions*, v.10,May 1978.pp.40+.

BRILL, Alan E. 'Realities in computer security'. *Armed forces comptroller*, v.21,Oct.,1976.pp.14-15.

BUND, Melvin. 'Security in an electronic data processing environment'. *CPA Journal*, v.45,Feb.,1975.pp.33-5.

'Bureaucrat apathy blamed for computer crime'. *Bus. Insur.*, v.10, Aug.9,1976.p.85.

BURGER, A.D. 'EDP audit: Don't forget the user'. *The Internal Auditor*, Feb.,1978.pp.20+.

BURKE, E.L. Discovering illicit computer usage. 12th IEEE Computers Society International Conference on Computers the Next 5 Years. (Digest of papers), San Francisco,Calif.,USA,Feb.24-26, 1976(New York,USA:IEEE 1976),pp.178-80.

BURKE, J. 'EFT: more security, not less'. *Banking*, v.69,Jan.,1977. p.37.

BURN, Christopher 'Auditing the computer-a time for reappraisal'. *Accountant*, v.172,Jan.30,1975.pp.131-3.

BURROW, Brian 'Where has all the data gone?'. *South African Chartered Accountant*, v.12,Feb.,1976.pp.53-4.

'Business is lucrative prey for thieves'. *Office*, v.84,Oct.,1976. pp.48+.

CAMERON, M. 'The awesome power of the computer crook'. *Insurance Record of Australia and New Zealand*, v.2,Aug.,1977.pp.287-289.

CAMERON, M. 'Crime in, crime out'. *Canadian Banker and ICB Review*, v.84,May 1977.pp.8-11.

CAMPBELL, Voin R. 'Privacy and security in local government info-systems'. *Infosystems*, v.23,Dec.,1976.pp.31-34.

'Canadian computer audit guidelines'. *Institute of Chartered Accountants*, Dec.,1976.p.418.

CARROLL, J.M. 'Detection of computer crime'. 4th Canadian conference on Info.Science on Info. Services in Canada, London, Ontario, Canada. *Canadian Assoc. Information Science*, May 11-14, 1976. pp.203-10.

CAMPISE, James A. 'Risk assessment and contingency planning'. *EDP Auditor*, Aug.,1977.pp.16-17,19.

CHAMBERS, A.D. 'Computer fraud and abuse'. *The Computer Journal*, Aug.,1978.pp.194+.

CLEVELAND, S. Thomas 'Strict controls help forestall wrongdoing and prevent errors'. *Newspaper controller*, v.30,Oct.,1976. pp.6-7.

CLUFF, E. 'The three faces of security'. *Computer Management*, May, 1978.pp.23,25-6.

COLE, G.D. *Design alternatives for computer network security.* Wash., National Bureau of Standards, 1978.

'A communications security checklist'. *Computer security,* Jan./Feb., 1978. Supplement.

'Computer abuse'. N.Y., Practising Law Institute, 1975.

'Computer abuse, 1976'. N.Y.,Practising Law Institute, 1976.

'Computer crime'. *Mechanical Engineering,* v.99,Nov.,1977.pp.76-77.

'Computer fraud'. *Accountant,* v.176,Feb.10,1977.pp.167-8.

'Computer fraud:growing retail menace'. *Chain Store Age Executive,* v.54,June,1978.pp.27-30.

COLE, R.B. 'Crime in business'. *SAM Advanced Management Journal,* Spring 1978.pp.17-23.

'Computer frauds - are they a manageable risk'. *Accountancy,* Oct., 1976.pp.78-79.

'Computer frauds build interest in security'. *Editor & Publisher,* v.109,May 29,1976.pp.9+.

'Computer frauds cost governemt $2M'. *Electronic News,* v.21,May 10, 1976.p.54.

'Computer nightmare'. *Economist,* v.262,Feb.12,1977.pp.103.

'Computer-related crimes(Federal agencies)EDP *Analyzer,* v.15,June, 1977.pp.3-5.

'Computer-related fraud'. *CPA Journal,* v.45,June,1975.pp.61-2.

'Computer security hardware devices & services'. *Edpacs,* v.4,March, 1977.pp.1-10.

'Computer security systems and services'. *Computing surveys,* no.6, pt.6,Dec.1977,pp.2-6.

'Computers and privacy, 4. (Computer world)'. *Certified accountant,* v.64,June,1977.pp.209-10,222.

'Computer's private eye'. *Economist,* v.261,Oct.30,1976.p.18.

'Congress goes after computer crime'. *Computer law and tax report,* v.4,Oct.,1977.pp.1-3.

'Control of computer techniques'. *CIPFA Audit Bulletin,* June,1976. pp.5+.

'Control system helps secure Times computers'. *Infosystems,* v.25, April,1978.pp.106+.

CONSTANZO, Louis Joseph 'What about data security'. *Motor freight controller,* Feb.,1976.pp.4-5.

COURTNEY, R.H. 'Horror stories funny, but! ' *Datamation,* v.21,Nov., 1975.pp.137-8.

COURTNEY, R.H. 'A systematic approach to data security'. *Informatie,* Sept.1975.pp.405+.

CRANWELL, B. 'Appraising internal audit'. *Public finance and accountancy*, July,1978.pp.355-357.

'Crime in a cashless society'. *Futurist*, v.10,June,1976.p.132.

CROCKFORD, N. 'A guide to risk management'. *Foresight*, Oct.,1976. p.47;Nov.,1976.p.47;Jan.,1977.p.42;Feb.,1977.p.46;March, 1977.p.48;April,1977.p.49+.

'Cryptic standard'. *MBA/Masters in Business Administration*, v.12, Feb.,1978.p.8.

'Cryptically yours'. *Economist*, v.266,Feb.4,1978.p.92.

'Cryptography and data communications'. *Infosystems*, v.22,July,1975. pp.28-30.

CURREY, J.P. 'Planning for disaster recovery'. *Infosystems*, v.25, March,1978.pp.64-69.

DANNER, L. 'Management aspects of the IBM data security study'. *Data management*, v.12,Sept.,1974.pp.39-42.

Datamation Magazine (Firm). 'Trends in computer room security'. Marketing Research Dept., Greenwich, Conn.,1974.

DAVIS, A. LEONARD 'Computer security and you'. *Accountancy*, v.86, Sept.,1975.p.80.

DAVIS, James R. 'Computer controls:a different emphasis preventing errors or fraud by implementing passive controls which include: documentation, organizational independence, and audit trails'. *National Public Accountant*, v.22,June,1977.pp.10-14.

DAVIS, R.M. 'Approaches to privacy and security in computer systems'. *National Bureau of Standards*, Wash.,1975.

DE HAAN, S. 'EDP security on a budget'. *Journal of Systems Management*, Jan.,1978.p.30.

DEMITRIADES, Paul B. 'Administrative secrecy and data privacy legislation'. *Journal of Systems Management*, v.27,Oct.,1976,pp.24-9.

DENT, I. 'Legislation proposed against computer fraud'. *The Credit World*, v.66,Feb.,1978.p.11.

DEVLIN, Gerald W. 'Internal control is not optional'. *Management Accounting*, (NAA), v.57,Aug.,1975.pp.49-51.

DIAL, O. Eugene 'Privacy, security, and computers:guidelines for municipal and other public information systems'. *Praeger*,1975.

DOMINGUES, K.V. 'Practical applications in the use of audit software'. *Interpreter*, v.35,Oct.,1976.pp.29-31.

DRYER, D. 'Protecting distributed processing'. *Security Gazette*, March,1978.pp.82+.

DE GOUW, Chris. 'Data processing crimes'. *Edpacs*, v.5,Jan.,1978. pp.1-8.

EDP Auditors Association. 'Control objectives'.*Hanover*, Park., Ill., v. 1,1975.

EDP Security. 'A perspective for management'. *Coopers & Lybrand Newsletter*, v.19,Dec.1977.

'EDP Security Guidelines'.*The Australian Computer Journal*, Mar.1976. pp.25+.

ELLISON, Ray. 'Changing face of the fraudsman'. *CPA Journal*, v.46, Jan. 1976.pp.5-6.

ELLISON, J.R. 'Computer risks'. *Foresight*, June 1978.pp.13+.

ELLISON, R. 'Computer security'. *Computing Europe*, Aug.14,1975.p.12.

EMENS, K.L. 'Mailing list security'. *Edpacs*, v.5,April,1978.pp.1-6.

ENTICKNAP, N. 'Should you bet your company? Security'. *Data Processing*, v.18,no.5,July/Aug.1976.pp.41-2.

Erfassungsschutz:der Burger in der Datenbank:zwischen Planung und Manipulation, Stuttgart,Deutsche Verlags-Anstalt, 1975.

Exploring privacy and data security costs:a summary of a workshop:a report of the NBS Workshop on Privacy and Data Security Costs, February 20,1975.

FABVRE, M. 'An experimental security audit of the clearing computer in the Banque de France'. *Convention Informatique*, 1975.

FARR, M.A.L. 'Security for computer system'. Manchester,National Computing Centre, 1972.

FARR, Robert. 'Electronic criminals'.New York,McGraw-Hill, 1975. p.194.

FLATO, L. 'EFT and crime,electronic funds transfer'. *Computer decisions*, v.7,no.10,Oct.1975.pp.30-3.

FLATO, L. 'Navy sinks 1108'. *Computer decisions*, v.8,no.7,July,1976. pp.35-6.

'Fight to foil computer fraud'.*Nation's business*, v.68,March,1976. pp.8D+.

FINE, L. 'Computer disaster prevention'. *Data Processing*, April, 1978.pp.12+.

FINE, L.H. 'Computer disaster planning and testing'. *Systems(S.Africa)*, v.8,no.3,March,1978.pp.12,14+.

FINE, L.H. 'Computer disaster prevention-a new approach'. *Data processing*, v.20,no.4,April,1978.pp.12+.

FINE, Leonard H. 'Computer security-experience with the total security concept'. *South African chartered accountant*, v.12,April,1976.pp.113-14.

FINE, L. 'A computer security policy'. *Management*, Jul./Aug., 1977.pp.46+.

FINE, Leonard H. 'Defining a computer security policy'. *South African chartered accountant*, v.13,Nov.1977.pp.399+.

FINE, Leonard 'How to create a computer security policy'. *Management*, v.24,Jul./Aug.,1977.pp.46-8.

FINE, L. 'A new approach to computer disaster planning:the total security concept'. *South African chartered accountant*, v.14, March 1978.pp.97-101.

FINE, L.H. 'The total computer security concept'. *CA Mag.*,v.111, no.8,Aug.1978.pp.59-63.

FIRNBERG, D. 'Your computer in jeopardy'. *Computer decisions*, v.8, no.7,July 1976.pp.28-30.

'First pass at privacy laws given an A for adequate'. *Datamation*, v.21,Feb.1975.pp.71+.

FITZGERALD, Jerry 'Developing and ranking threat scenarios'. *Edpacs*, v.6,Sept.,1978.pp.1-5.

FITZGERALD, J. 'EDP risk analysis for contingency planning'. *Edpacs*, v.6,Aug.1978.pp.1-8.

'Fourth conference on computer audit'. *Edpacs*, v.2,March 1975.pp.10-19.

FREESE, Jan. Data och livskvalitet:om dataregister och deras anvandning-Stockholm:Liberforlag:Jurist- o.samhallsvetareforb, 1976.

GAIT, J. 'Easy entry:the password encryption problem'. *Oper.Syst. Rev.*, v.12,no.3,July,1978.pp.54-60.

GATES, P.O. 'How can accountants and auditors prevent computer fraud'. *The government accountants journal*, v.27,Summer 1978,pp.10-15.

GELLMAN, H. 'Statistical data banks and their effects on privacy:a study for the Privacy and Computers Task Force'. *Dept. of Communications*, 1973.

GELLMAN, H.S. 'Using the computer to steal'. *Journal of systems management*, v.25,Oct.1974.pp.28-32.

GENTILE, E.A. 'Maintaining internal integrity of on-line data bases'. *Edpacs*, v.4,Feb.1977.pp.1-14.

GILDERSLEEVE, Thomas R. 'Who owns the data?' *Infosystems*, v.23,Oct. 1976.pp.70-72.

GILSON, Milo, 'Computer assisted fraud - who gets the axe?' *Data Management*, v.13,April 1975.pp.22-3.

GLADNEY, H.M. 'Administrative control of computing service'. *IBM Systems journal*, v.2, 1978.pp.151-78.

GLASER, G. 'Economics of security for computer systems'. *Office*, v.81,Jan.1975.pp.60+.

GOETZ, Martin A. 'Software protection:you bet your company'. *Infosystems*, v.24,July 1977.pp.60+.

GOLDSTEIN, Robert C. 'The cost of privacy:operational and financial implications of databank-privacy regulation'. *Honeywell information systems*, 1975.

GOLDSTEIN, Robert C. 'Costs of privacy'. *Datamation*, v.21,Oct.1975. pp.65-9.

GORMAN, J. 'Computer capers'. *Datamation*, v.23,no.3,March 1977. pp.105-6.

GOTLIEB, C. 'Systems capacity for data security:a study for the Privacy and Computers Task Force'. *Dept. of Communication*, 1972.

GOTTHEIMER, D. 'Those hidden opportunities for computer crime'. *Administrative Management*, v.39,Jan.1978.pp.65-6+.

GRAPE, Enrique 'Comprehensive security in data processing systems: the state of the art'. Urbana-Champaign, 1975.

Great Britain. Home Dept. Computers, safeguards for privacy.London, 1975.

GREEN, Gion 'Introduction to security'.*Security World publication*, 1975.

GREGGAINS, D. 'Timesharing security'. *Computing Europe*, Aug.14, 1975.p.13.

GRIHALVA, Richard A. 'Auditing load libraries'. *Edpacs*, v.5,Oct., 1977.pp.1-6.

GRONNING, T.G. 'Data security and the financial community'. *Sloan Management Review*, v.15,Sept.1974.pp.69-82.

'Growing threat to computer security'.*Business week*, Aug.1,1977. pp.44-5.

'Guarding against computer fraud'.*Banking*, v.68,April 1976.pp.36+.

'Guidelines for establishing a computer security program'.*Computer Security Institute*, Hudson.

HALFORD, D. 'Risk analysis'. *Foresight*, Jan.1978.pp.9+.

HALL, T. 'The electronic office'. *Computing Europe*, v.17,Aug.1978. pp.16-17.

HAMILTON, Peter 'Computer security'. Philadelphia, *Auerbach Pub.*, 1973.

HEMPHILL, C.F. 'Security procedures for computer systems'.

HEINRICH, F. 'The network security centre : a system level approach to computer network security'.Wash., *National Bureau of Standards*, v.2,Jan.1978.pp.55.

HMSO. Computers: Safeguards for Privacy. London, HMSO, 1975.

HMSO. Computers & Privacy. London, HMSO, 1975.

HOFFERBERT, R.I. 'Social science archives and confidentiality'. *American Behavioural Scientist*, v.19,March 1976.pp.467-83.

HOFFMAN, L.J. 'Modern methods for computer security and privacy'. Englewood Cliffs, N.J., Prentice-Hall, 1977.

HOFFMAN, L.J. 'Security and privacy in computer systems'. N.Y., Wiley, 1974.

HOLLIS, Gerald 'Basics of computer security(accountants and the computer)'. *Accountancy*, v.88,Jan.,1977.pp.108,111-12,114.

HOLLIS, G. 'Computer security'. *Accountancy*, Jan.,1977.pp.108+.

HOLMER, Walter Datasakerhet : produktion - Lund:Studentlitteratur, 1975.

HORWITZ, Geoffrey B. 'Computer audit and security'. *South African chartered accountant*, v.1[illegible],Nov.,1975.pp.371-6.

HOSMAN, Paul 'The dedicated mutual aid agreement'. *Computer security*, Nov./Dec.,1977.

HORNE, J.M. 'EDP controls to check fraud'. *Management accounting*, v.56,Oct.,1974.pp.43-6.

'How secure are your computers?' *Industry week*, v.186,Sept.,22, 1975.pp.40+.

'How to stop the computer embezzlers'. *Rydges*,v.51,Feb.,1978.pp.70-72.

HOWE, Eric 'Attitudes to computer security'. *Accountant*, v.174, Feb.,12,1976.pp.185-6.

HOWE, E.J. 'Computer security-public and user attitudes'. *The Internal Auditor*, v.35,April,1978.pp.79-85.

HOYT, D.B. 'The computer as a target for the industrial spy'. *Assets protection*, v.1,Spring,1975.pp.41-7.

HOYT, D. *Computer security handbook*, N.Y., MacMillan, 1974.

HSIAO, D.K. 'Computer security and privacy'. *Naval research review*, v.31(1),1978.pp.21-26.

HUCK, S.L.M. 'How elections are stolen'. *American opinion*, v.19, Nov.,1976.pp.1+.

HUNTER, G. 'DP error and fraud-a[illegible]d what you can do about it'. *Price Waterhouse review*, v.21,[illegible].2,Aug.,1976.pp.3-11.

'The importance of EDP audit and control'. *EDP analyzer*, v.15,no.6, June,1977.pp.1-13.

'IBM continues EDP security study'. *Management adviser*, v.11,July, 1974.pp.11-12.

International Business Machines Corporation. Data security and data processing. White Plains,N.Y.,1974.

IBM 'DP division offers encryption products line'. *Electronic News*, v.22,Dec.12,1977.pp.20+.

Illinois, Secure automated facility environment project. Springfield, 1974.

'Inside operators'. *National underwriter(Property edition)*, v.78, July 26,1974.p.16.

JACOBSON, P.V. 'Finding hidden computer crime'. *Security management*, v.22,April,1978.pp.16-18.

JANCURA, E.G. Audit & control of computer systems.

JANCURA, G. 'Privacy and the computer. Electronic data processing. *Woman CPA*, v.38,July 1976.pp.16-18.

JEBSON, A. 'The computer in audit'. *Accountancy*, June, 1978.pp.95+.

JONES, G. Hunter. 'DP error and fraud-and what you can do about it'. *Price waterhouse review*, v.21,no.2,1976.pp.2-11.

JONES, G.H. 'EDP error and fraud'. *Price waterhouse review*, v.2, 1976.pp.3+.

JONES, G. Hunter. 'Guarding against computer fraud'. *Banking*, v.68, April 1976.pp.36,57.

JOPSON, Debra. 'Computer criminals'. *National times*, v.22, July 1977.pp.18-23.

JOSEPH, Anthony M. 'Computer fraud...and sales audit.Systems digest'. *Retail control*, v.45,Oct.1977.pp.49-57.

JOSEPH, Anthony M. 'Preventing computer fraud'. *Retail control*, v.45,March 1977.pp.55-64.

KAPNICK, H. 'Responsibility and detection in management fraud'. *CPA Journal*, May 1976.pp.19+.

KELLER, G.W. 'Security and the computer'. *Electron. Electro-Optic and infrared countermeasures*, v.1.no.3.July 1975.pp.34-6.

KELLEY, Neil D. 'Protecting your computer system'. *Infosystems*, v.24,Dec. 1977.pp.39-41.

KOEHN, H.E. 'Do vital records need a fortress?' *Journal of systems management*, v.25,Sept. 1974.pp.32-4.

KOGITZ, S. 'Privacy and data security. The DP manager's viewpoint'. *Can.datasyst.*, v.10,March 1978.pp.36-7,40.

KOTOWSKI, M. 'Identification of the user in multiaccess systems'. *Informatyka, (Poland)*, v.12,no.6,June 1977.pp.3-5.

KRAUS, W. 'Auditability of EDP-assisted information systems'. *European journal of accountancy*, April 1978.pp.80+.

LANCASTER, Hal. 'Desktop deception:r[illegible] of minicomputers, ease of running them facilitate new frauds'. *Wall St. Journal*, v.190,Oct.5,1977.pp.1+.

LEEPSON, M. 'Computer crime'. *Editorial research reports*, Jan.6, 1978.pp.3-20.

LEIBHOLZ, S.W. 'Users' guide to computer crime:its commission, detection & prevention'. *Chilton*, Oct.,1975.

LENZ, Matthew. 'Protecting the computer center'. *Risk management*, v.23,Aug.1976.pp.25-6,28,30,48,50.

LIENTZ, Bennet P. 'Vulnerability of computer auditing'. *CPA Journal*, v.47,March 1977.pp.17-21.

Life Office Management Association.'Basic audit and control considerations in the electronic data processing environment'. *Financial planning and control report*, New York, no.32,1975.p.76.

LOBEL, Jerome, 'Computer security'. *Information systems handbook*, Homewood, Ill., 1975.pp.832-42.

LOBEL, J. 'Planning a secure system'. *Journal of systems management*, v.27,no.7,July,1976.pp.14-19.

LORD, Kenniston W. 'Data center security: a case for the private eye'. *Infosystems*, v.23,Dec.1976,pp.30-1,33.

LOWE, R.L. 'Auditing the corporate information system'. *CPA Journal*, v.47,Nov.,1977.pp.35-40.

McCARTHY, P. 'Electronic data processing audits and the insured S and L (savings and loan association)'. *Federal Home Loan Bank Board Journal*, v.11,May,1978.pp.18-21.

McCAULEY, E.J. 'Highly secure attributed based file organization'. (Center Advanced Computation, Univ.of Illinois, Urbana,Il., USA). 2nd USA-Japan Computer Conference Proceedings, Tokyo, Japan, Aug.26-28,1975 (Montvale, N.J.,USA: AFIPS 1975), pp.497-501.

McGUIRE, Patrick T. 'EDP auditing - Why? How? What?' *Internal Auditor*, v.34,June,1977,pp.27-34.

McKNIGHT, G. 'Computer crimes'. *Walker*, 1974.

MAIR, William C. 'Computer control and audit'. *Institute of Internal Auditors*, 1976.p.489.

MAIR, W., WOOD, D., DAVIS, K., 'Computer control and audit necessity'. *Computers and People*, v.25(II),1976.pp.18-21.

MANOLA, F.A., 'Data security implications of an extended subschema concept'. (Naval Res. Lab.,WASH., USA). 2nd USA-Japan Computer Conference Proceedings, Tokyo, Japan,Aug.,26-28,1975. (Montvale, N.J., USA: AFIPS 1975),pp.481-7.

MARINER, E.T. 'Can your computer be used against you?' *Hotel and Motel Management*, v.192,April,1977.pp.28-9.

MARSH, Rolf, 'Making data more secure'. *Datamation*, v.22,Oct.,1976. pp.67-9.

MARTELLA, G. 'Security techniques in information systems: an overview'. *Systems*, v.6,no.3,March,1976.pp.6-7,9-12.

MARTIN, J. 'Computer database organization'. Englewood, Cliffs,N.J., *Prentice-Hall*, Jan.,1976.p.27,

MARTIN, J. 'Future development in telecommunications'. Englewood, Cliffs, N.J., *Prentice-Hall*, 1977.

MAYREND, G.R., 'Guide to EDP control'. *Journal of Systems Management*, v.29,Feb.,1978.pp.16-17.

MEISSNER, P. 'Preventing unauthorized access'. *Data Processing*, Jul./Aug.,1977.pp.42+.

MENKUS, Belden 'Management's responsibilities for safeguarding information'. *Journal of systems management*, v.27,Dec., 1976.pp.32-8.

MENKUS, Belden 'New perspective on data processing risk management'. *Risk management*, v.23,Aug.,1976.p.62.

METHODIOS, I. 'Internal controls and audit'. *Journal of systems management*, v.27,June,1976.pp.6-14.

MEYERS, Gerald Edwin 'EDP related fraud'. (Questions for the experts). *EDP auditor*, Winter,1976.p.22.

MILLIGAN, Robert H. 'Management guide to computer protection'. *Journal of systems management*, v.27,Nov.,1976,pp.14-18.

MILLS, L. 'Security'. *The office*, Aug.,1977.pp.25-31.

'Misappropriation in the computer room'. *Rydges management service*, v.12,15 March,1978.pp.17-20.

MORRIS, E. 'Auditing and the computer'. *Computer management*, v.12, no.11,Feb.,1978.pp.11+.

MULDER, L. 'Computer security: a contradiction of terms?' *Government data systems*, v.7,no.3,May/June,1978.pp.31-2.

MULLIN, M.A. 'Computer security - the human element'. *South African chartered accountant*, v.13,Aug.,1977.pp.257-9.

MURDOCK, G.W. 'Computer security in a multi-user environment'. *S. Dakota business review*, v.34,Aug.,1975.pp.3+.

MYERS, E. 'Computer criminals beware!' *Datamation*, v.21,Dec.,1975. pp.105+.

MYERS, E., 'Computer security: each case is different'. *Datamation*, v.21,April,1975.pp.107-9.

MYERS, E. 'Credit checking; an unsophisticated computer crime'. *Datamation*, v.22,Nov.,1976.pp.146+.

MYERS, E. 'Privacy: a political issue'. *Datamation*, v.24,May,1978. pp.261-3.

MYERS, E. 'Security: the only means to privacy'. *Datamation*, v.23, May,1977.pp.240-2.

NATIONAL COMPUTING CENTRE 'Where next for computer security'. *National computing centre publ.*, Feb., 1975.p.143.

NATIONAL FIRE PROTECTION ASSOCIATION 'Protection of electronic computer/data processing equipment'. Boston, 1972.p.33.

NATIONAL STUDY GROUP ON THE SECURITY OF COMPUTER-BASED SYSTEMS 'Where next for computer security?' *NCC Publications*, 1974.

NEWSOME, E. 'Computer security'. *Accountancy age*, Sept./Oct.,1974.

1977 Carnahan conference on crime countermeasures. Lexington,KY,USA., Univ. Kentucky, 6-8 April,1977.

NORMAN, Adrian 'Computer frauds - are they a manageable risk?' *Accountants' journal*, v.56,May,1977.pp.134-7.

NOTTINGHAM, C. 'Conceptual framework for improved computer audits'. *Accounting and business research*, v.6,no.22,Spring 1976. pp.140-8.

NYCUM, S. 'Legal aspects of computer abuse'. 12th IEEE Computers Society International Conference on Computers the Next 5 Years. (Digest of papers), San.Francisco, Calif.,USA, 24-26 Feb.,1976(New York, USA: IEEE 1976),pp.181-3.

O'CONNELL, S. 'Distributed processing'. *Computer weekly*, 25 Aug., 1977.pp.15+.

OKKERSE, P. 'Computer crime'.*The chartered accountant in Australia*, April,1978.pp.34+.

O'MARA, John C. 'Computer security: a risk management blind spot'. *Risk management*, v.23,Aug.,1976.pp.22-4.

O'MARA, J.C. 'Security for computer facilities'. *Office*, v.82, Dec.,1975.p.50.

Organization for Economic Cooperation and Development. Policy issues in data protection and privacy : concepts and perspectives : proceedings of the OECD seminar 24-26th June,1974-Paris : Organisation for economic co-operation and development;Wash., USA,1976.

ORR, Kenneth T. 'Data security and privacy: phase two'. *Infosystems*, v.23,Feb.,1976.pp.34-5.

O'SULLIVAN, E.'The equity funding scandal'. *Accountancy Ireland*, June,1975.pp.21+.

PALMER, E.J. 'Eleven fifty-seven and counting'. *Data management*, v.15,Oct.1977.p.12.

'Pansophic's new PANEXEC manages program libraries, security, for 360/370 users'. *Data management*, v.16,Feb.1978.p.57.

PANTAGES, Angeline 'New headache for international DP'. *Datamation*, v.23,June,1977.pp.115+.

PANTAGES, Angeline 'Price of protection'. *Datamation*, v.22,March, 1976.pp.141,144.

PARKER, D.B. 'Computer abuse'. *National science foundation*, 1973.

PARKER, D.B. 'Computer and data abuse'. 12th IEEE Computers Society International Conference on Computers the Next 5 Years. (Digest of papers), San Francisco, Calif.,USA, 24-26 Feb.,1976(New York, USA: IEEE 1976),pp.184-6.

PARKER, D.B. 'Crime by computer: startling new kinds of million dollar fraud, theft, larceny and embezzlement'. N.Y., *Scribner*, 1976.

PARKER, D.B. 'Equity Funding - a computer fraud?' (In *Crime by computer*, 1976.pp.118-74.)

PARKER, D.B.'Look at computer fraud and embezzlement in banking'. *Magazine of bank administration*, v.52,May,1976.pp.18-23.

PARKER, D.B. 'Round-down fraud'. *Bankers magazine*, v.160,Spring, 1977.pp.28-30.

PARKER, D.B. 'What every executive should know about making computers safer to use'. *Computer security institute*, Northboro, Mass.

PARRY, James 'Computer theft: you may be the last to know'. *Canadian business*, v.49,May,1976.pp.63-4+.

PATRICK, R.L. 'AFIPS system review manual on security'. *American Federation of Information Processing Societies*, 1975.

PATRICK, R.L. 'Performance assurance and data integrity practices'. *National Bureau of Standards*, Wash., USA.,Jan.,1978.p.45.

PATRICK, R.L. 'Security systems review manual'. *AFIPS press*, v.27, Feb.,1975.

PEARSON, M.A. 'Minimum acceptable EDP accounting control standards'. *Massachusetts CPA review*, v.51,Nov./Dec.,1977.pp.7-9,38.

PERRY, W.E. 'Audit aspects of utility programs'. *Edpacs*, v.3,Oct., 1975.pp.1-8.

PERRY, W.E. 'Skills needed to utilize EDP audit practices'. *Edpacs*, v.5,Nov.,1977.pp.1-13.

PERRY, W.E. 'Systems auditability: friend or foe'. *Journal of accountancy*, v.145,Feb.,1978.pp.52-60.

PERRY, W.E. 'Using SMF as an audit tool - security'. *Edpacs*, v.3, Jan.,1976.pp.1-8.

PERSONAL RECORDS:procedures, practices, and problems:a study for the Privacy and Computers Task Force. Dept. of Communications,1973

POMERANZ, F. 'Securing the computer'. *CPA Journal*, v.44, June,1974. pp.23-6.

POPPA, R.P. 'Computers not really part of white collar crime wave'. *Computer digest*, v.13,no.1.,Jan.,1978.p.7.

PORTER, N. 'Security inside the EDP department'. *Computer weekly*, v.23,March, 1978.p.21.

PORTER, W.E, 'Privacy act of 1974: a look at it from a combined technical and legal perspective'. *Computers and people*, v.25,Dec.,1976.pp.10-13.

POUND, G.D. 'EDP auditing'. *Accounting and business research*, Spring 1978.pp.108+.

PRITCHARD, J. 'Computer security'. *Computer management*, June,1978. pp.9+.

PRITCHARD, J. 'Security of computer networks'. *Computing Europe*, 25th Aug.,1977.pp.14+.

'Privacy and the computer'. *Accountant*, v.175,July 8,1976.pp.36-7.

'Probe LA data bureau in wake of check theft'. *Electronic news*, v.19,Dec.23,1974.p.38.

Proceedings of papers presented at Computer Security 1974. Amstel Hotel, Amsterdam, 26-28 Feb., 1974 / conference organisers, the National Computing Centre, IFIP Administrative Data Processing Group (IAG). Manchester, *NCC Publications*, 1974.

'Protecting a vital part of the office-the computer'. *Administrative management*, v.39,March, 1978.p.71.

'Protection of computer rooms'. *Buro + EDV (Fed. Rep. of Germany)*, Sept.1977.pp.16+.

RABARTS, P. 'What auditor needs to know about fraud'. *Accountancy*, v.89,no.1024,Dec.,1978.pp.46-48.

RADCHUCK, R.P. 'EDP insurance'. *CA magazine*, Aug.,1978.pp.54+.

RANDALL, R. 'Computer fraud: a growing problem'. *Management Accounting*, v.39,April,1978.pp.61-4.

RANDALL, J. 'Industrial espionage'. *People & Profits*, Nov., 1975. pp.5+.

REED, Irving S. 'The application of information theory to privacy in data banks'. Santa Monica, Rand, 1973.

REEVE, J.T. 'Lessons from equity funding'. *The Internal Auditor*, Oct.,1976.pp.20+.

RENEAU, J.H. 'Auditing in a data base environment:controls over access to data represent a major difference between file systems and data base systems'. *Journal of accountancy*, v.144,Dec.1977.pp.59-65.

RICHARDSON, Dana R. 'Issue of privacy.(EDP)'. *California CPA quarterly*, v.44,June,1976.p.26.

RILEY, John H.C. 'Computer fraud and embezzlement'. *Newspaper controller*, v.30,Oct.1976.p.6.

'Risk management: preparing for disaster'. *The Big Byte*, v.5,Sept., 1977.

'Risk managers urged for curbing fraud'. *Datamation*, v.22,June,1976. pp.155+.

RITTENBERG, L.E. 'The roles of internal and external auditors in auditing EDP (electronic data processing) systems'. *Journal of accountancy*, v.144,Dec.,1977.pp.51-8.

RITTERSBACH, G.H. 'Toward computer security'. *Management controls*, v.22,Oct./Nov.,1975.pp.158-65.

ROBERTS, J.G. 'Cash dispensers trap criminals'. *Burroughs clearing house*, v.59,Oct.,1974.pp.46+.

RODDAM, P.L. 'Auditors and computers'. *Accountant*, v.177,Aug.,1977. pp.168-9.

ROBERTSON, J. 'Oil computer leaks (FEA system)'. *Electronic news*, v.20,July,1975.p.10.

ROMNEY, Marshall 'Detection and deterrence: a double barreled attack on computer fraud'. *Financial executive*, v.45,July,1977. pp.36-41.

ROMNEY, Marshall 'Fraud and EDP'. *CPA Journal*, v.46,Nov.,1976. pp.23-8.

ROSENSTEIN, J. 'Computer security'. *Perspective*, USA., Spring/ Summer 1977.p.16.

ROSENSTEIN, J. 'Computer security for ripoffs-goofs-other maladies'. *Retail control*, v.45,Sept.1977.pp.49-55.

ROTHMAN, M.B. 'High stakes in computer crimes'. *Stores*, v.60, Feb.,1978.pp.39-40+.

ROYAL, R.F. 'Embezzlement, larceny and fraud'. *The Office*, Dec., 1976.pp.53+.

RUDER, B. 'An analysis of computer security safeguards for detecting and preventing intentional computer misuse'. *National Bureau of Standards*, Wash., USA., Jan.,1978.p.71.

RUDER, B. 'Developing an EDP risk analysis plan'. *Risk management*, v.25,March,1978.pp.12-17.

RUSLEY, Roger L. 'Embezzler vs. computer: don't bet on the computer'. *Medical economics*, v.53,Sept.20,1976.pp.156-7,161,164.

SANDER, L. 'Privacy, security, and ciphers'. *Data processor*, v.21, Jan.,1978.pp.2-6.

SCHWARTZ, L. 'Ribicoff bill would punish burglar use of computer'. *Electronic news*, v.22,June 27,1977.p.8.

SCOMA, Louis 'Data center security'. *Data management*, v.13,Sept., 1975.pp.19-21.

SCOMA, L. 'The EDP auditor'. *Data management*, May,1977.pp.15-17.

SEARCH GROUP Standards for security and privacy of criminal justice information / submitted by SEARCH Group,Inc.-Sacramento, Calif. : The Group, 1975.

'Security units protect computer data'. *Editor & Publisher*, v.111, Jan.14,1978.p.35.

SHANKAR, K.S. 'Total computer security problem'. *Computer*, v.10, June,1977.pp.50-62.

SHARRATT, J. 'Data control guidelines'. *NCC Publications*, 1974.

SIEGHART, P. 'Privacy & Computers'.

SMEJDA, Hellena 'Build controls into system for EDP security'. *Hospital financial management*, v.31,March,1977.pp.34-7,40.

SMITH, A.W. 'Data processing security: a commonsence approach'. *Data management*, May,1977.pp.7-13.

SMITH, R.C. 'Equity funding: implications for auditing and data processing'. *Edpacs*, v.2,Oct.1974.pp.1-7.

SMITH, R.M. 'Communications, auditing stressed at eleventh annual AICPA computer conference'. *Journal of accountancy*, v.140, July,1975.pp.24,26,28,30,32.

'So far, so fair; computer privacy'. *Economist*, v.257,Dec.,1975. p.22.

SOLOMON, Richard J. 'Encryption controversy'. *Mini-micro systems*, v.11,Feb.,1978.pp.22,24-6.

SPRAGUE, Richard E. 'Computer professionals: what their social concerns need to be'. *Computers and people*, v.24,Feb., 1975.pp.36-9.

SRINIVASAN, C.A. 'Computer system security and auditing implications'. *National public accountant*, v.23,Jan.1978.pp.20-4.

STADLER, Norbert 'Datensicherung durch Organisation : Voraussetzung d.'- Freiburg im Breisgau : Haufe, 1975.

STANLEY, Philip 'Computer crime: let the honest manufacturer beware'. *Manufacturer's monthly*, v.18,May,1978.pp.16-17.

STEGUWEIT, H.D. 'Insurance against computer abuse'. *Rationalislerung, (Fed.Rep.of German)*, Feb.,1975.pp.44+.

STERN, L. 'Contingency planning: why? how and how much?' *Datamation*, v.20,Sept.,1974.pp.83+.

STERN, L. 'Security for your computer facility'. *The Office*, v.88, Aug.,1978.pp.18-20,44.

STONE, M.G. 'Data-bank fiasco'. *Pol Q*, v.47,Oct.,1976.pp.468-73.

STONE, R. 'Some security and integrity controls in small computer systems'.(Accounting and EDP). *Journal of accountancy*, v.141, Feb.,1976.pp.36,38,40.

STONE, R.L. 'Who is responsible for computer fraud?'(Accounting and EDP). *Journal of accountancy*, v.139,Feb.,1975.pp.35-9.

STONE, W.E. 'Computer fraud'. *South African chartered accountant*, v.11,Oct.,1975.pp.333-4.

STONE, W.E. 'Internal control for EDP systems'.*South African chartered accountant*, v.12,Aug.,1976.pp.263-5,267-8.

STROBIN, Edward A. 'Computer security - POS terminal controls'. *Retail control*, v.44,Dec.1975.pp.38-47.

STROTHER, Robert, 'Crime by computer'. *Chartered accountant*, (India), v.25,May,1977.pp.739-40.

SULCAS, P. 'The working papers of a computer auditor'. *Accountancy*, Nov.,1977.pp.134+.

SYKES, David J. 'Protecting data by encryption'. *Datamation*,v.22, Aug.,1976.pp.81,84-5.

'Task force on privacy and computers'. *Privacy and computers*, Ottawa, Information Canada, 1972.

'They should be paranoid'. *Datamation*, v.23,Sept.,1977.pp.29-30.

'This month's case study:avoiding the fraud traps in computers'. *Rydges management service*, v.11,March 15,1977.pp.7-9.

THORNE, J.P. 'Computer abuses: its implication for accounting education'. *Collected papaers of the 27th annual meeting, Richmond, Va.*, 1975.pp.69-73.

THORNE, J.P. 'Control of computer abuses'. *Journal of accountancy*, v.138,Oct.,1974.pp.40+.

THORNTON, C. 'Are you safe'. *Computer management*, June 1978.p.15.

TOBIN, L.E. 'Secure information via off-site retention'. *Risk management*, v.23,Aug.,1976.pp.56,58.60.

TOMESKI, E.A. 'Behavioural issues and the computer'. *Personnel*, July/Aug.,1978.pp.66+.

TOMESKI, E.A. 'Computers create social issues'. *Journal of systems management*, v.27,Feb.,1976.pp.30-3.

TUDOR, Gary A. 'Protection of data, information and data processing resources: new rules, requirements and responsibilites for management, EDP auditing and legal staff'. *EDP auditor*, Spring 1976.pp.12-19. (part one).

TUDOR, Gary A. 'Protection of data information and data processing resources'. *EDP auditor*, Summer 1976.pp.20-7. (part two).

TUDOR, Gary A. 'Protection of data information and data processing resources'. *EDP auditor*, Fall 1976.pp.18-23. (part three).

TURN, R. 'Privacy and security in personal information databank systems' : prepared for the National Science Foundation, Santa Monica, Ca., 1974.pp.97-104.

TURN, R. 'Privacy protection and security in business computer systems'. *Atlanta economic review*, v.26,Nov./Dec.,1976. pp.24-30.

TUTT, G. 'Some important considerations in data communications'. *Data management*, v.13,Sept.,1975.pp.36-9.

TYRNAUER, Stuart 'Auditing computer program maintenance'. *Internal auditor*, v.34,Aug.,1977.pp.68-72.

UNITED STATES 'Approcaches to privacy and security in computer systems'. *National Bureau of Standards special publication*, March 4-5,1974.p.71.

UNITED STATES 'Managers need to provide better protection for Federal automatic data processing facilities, multiagency'. *General accounting office*, Wash.,1976

UNITED STATES National Bureau of Standards. Glossary for computer systems security. *U.S. Govt.Print.Office*, 1976.

UNITED STATES National Bureau of Standards.'Government looks at privacy and security in computer systems'. Dec.,1974.

UNITED STATES Senate. Com. on govt. operations. Problems associated with computer technology in federal programs and private industry: *Computer abuses*, 1976.

USPRICK S. 'The theory and practice of self-regulation'. *Dept. of communications*, Ottawa, 1973?

VANN, J. 'Insuring your computer'. *Computer management*, July/Aug., 1977.pp.17+.

VARGA, Joseph 'Safeguarding your computer resources'. *Cornell hotel and restaurant administration quarterly*, v.16,Nov.,1975. pp.56-60.

VERBOIS, A. 'Software security: an unresolved problem'. *Data Management*, v.12,Oct.,1974.pp.16-19.

VERNON. Lawrence J. 'Computer as an internal audit tool'. *Retail control*, v.45,Oct.,1976.pp.23-30.

VORIS, J. Walker 'How the computer can be used to commit fraud'. (Computer and you) *Practical accountant*, v.8,March/April, 1975.pp.63-4.

WAGNER, Charles R. 'Computer fraud: is it a problem?' *South Dakota CPA*, v.31,March/April 1977.pp.3-4.

WAGNER, Charles R. 'Methodology of computer fraud'. *South Dakota business review*, v.36,Aug.,1977.pp.7-9.

WALLER, Richard R. 'Computer fraud'. *Accountant*, v.173, October 2, 1975.pp.392-3.

WALLER, R.R. 'Security and computers'. *Accountant*, v.178,April 13, 1978.pp.500-1.

WALSH, John P. 'Computers, privacy, and the law'. *Australian accountant*, v.45,Oct.1975.pp.537-40,543-4.

WARDLAW, J.B. 'Auditing in a dispersed EDP environment'. *The Internal Auditor*, June 1977.pp.66+.

WARDLAW, John B. 'Security, control, and auditing in a dispersed data processing environment'. (EDP systems) *Internal Auditor*, v.34,June 1977.pp.66-73.

WARE, Willis H. 'Meet DPMA's computer sciences men-of-the year'. *Data management*, v.13,June 1975.pp.19-26.

WASSERMAN, Joseph J. 'Data security in an on-line computer environment'. *EDP auditor*, Fall 1974,pp.2-4,16-18.

WEBER, Ron. 'Audit perspective of operating system security'. (Accounting and EDP) *Journal of accountancy*, v.140,Sept.1975.pp.97-100.

WECHSLER, E.M. 'Burden is proving infidelity in computer crime'. *Business insurance*, v.10,July 12,1976.p.34.

WEISS, Harold 'Rebuttal to Equity Funding implications'. *Edpacs*, v.2,Oct.,1974.pp.8-11.

WESTALL, K. 'Can you spot the company crook'. *Chief executive(GB)*, June,1978.pp.20-1.

'What if they steal your computer?' *Management review*, v.67,June, 1978.p.6.

'Where the computer criminal can have a field-day'. *Data systems, (GB)*, March,1978.pp.24-5.

WHITESIDE, Thomas 'Annals of crime'. *The New Yorker*, v.53,Aug.,22 and 29,1977.

WHITESIDE, T. 'Dead souls in the computer'. *MBA/Masters in business administration*, v.12,May 1978.pp.33-4+.

WIENER, Hesh 'Why police states love the computer'. *Business and society review*, no.22,Summer,1977.pp.38-43.

WILKINSON, M. 'Beware your programmer!' *The financial times*, (UK), March 13,1978.

WILLIAMS, E. 'Scotland Yard and Home Office in all-out effort to fight crime by computer'. *Engineer*, v.246,March 9,1978.pp.12-13.

WILLIAMS, John W.O. 'Data banks: a cause for concern'. *Data Management*, v.13,July,1975.pp.24-8.

WILLMOTT, G.M.R. 'Security and privacy of data'.(Student roundabout). *Accountant (Eng.)*, v.172,Jan.16,1975.p.88.

WOLF, E.D. 'Computer security'. *Cooperative accountant*, v.28,Winter 1976.pp.27-39.

WONG, K.K. 'Computer disasters'. *Computing Europe*, v.7,April 1977. pp.8+14,10+.

WONG, K.K. 'A methodical approach to security'. *Data Processing(GB)*, v.18,no.5,July/Aug.,1976.pp.43-4.

WONG, K.K. 'Risk analysis and control - a guide for the D.P. manager'. *National computing centre*, 1978.

WOOD, H.M. 'Computer science and technology: the use of passwords for controlled access to computer resources'. Wash., U.S. Dept. of Commerce, 1977.

WOOD, H.M. 'The use of passwords for controlled access to computer resources'. *National Bureau of Standards*, Wash.,U.S.,May, 1977.

WOOLDRIDGE, S. 'Security standards for data processing'. *Lond., Macmillan*, June,1975.p.109.

WOOLF, Emile 'Lesson of Equity Funding - the ultimate indictment'. *Accountancy*, v.88,Jan.,1977.pp.30-3,36,38,40.

YAGGI, L.A. 'Reasonable need, environment determine security facilities'. *Data management*, v.16,May 1978,pp.52-6.

YOSHIMURA, T. 'A survey of some security fratures on Japanese data-base management systems'. 2nd USA-Japan Computer Conference Proceedings, Tokyo, Japan,Aug.26-28,1975.pp.502-5.

ZALUD, B. 'Chicken little fears of IBM security device meaningless to most business date processors'. *Data Management*, v.16, Feb.,1978.pp.60-1.